SRH-366

THE HISTORY

OF

ARMY STRIP CIPHER DEVICES

(JULY 1934 - OCTOBER 1947)

DECLASSIFIED per Sec. 3, E.O. 12356
by Director, NSA/Chief, CSS

[signature] Date: 2 March 1987

Reviewer's note: This document was sanitized for FOIA release in 1975 and is now being provided to Record Group 457 with additional, declassified information.

COPY 4

THE HISTORY OF ARMY STRIP CIPHER DEVICES

(JUL 1934 - OCT 1947)

ARMY SECURITY AGENCY
WASHINGTON, D. C.

1948

001

(308 pp.)

SECRET

HISTORY ASA (ARMY STRIP CIPHER DEVICES)

NOVEMBER 1948

~~SECRET~~

ARMY SECURITY AGENCY

WASHINGTON, D. C.

THE HISTORY OF

ARMY STRIP CIPHER DEVICES

Prepared under the Direction of the

CHIEF, ARMY SECURITY AGENCY

November 1943

002

~~SECRET~~

HISTORICAL NOTE

THE HISTORY OF ARMY STRIP-CIPHER DEVICES, the original draft of which was prepared in Methods Branch, Security Division, AS-83, is the second of a series of ASA Project Histories, the first volume of which, entitled THE HISTORY OF CIPAX, was issued in 1947.

The documents referred to in the footnotes of the present volume under File AS-80 are located in the Information and Records Section, AS-80A.

Numerous references have been made in the text of this history to Mr. William F. Friedman. This is due, not only to the position Mr. Friedman held in the War Department Plans and Training Division as Chief, Codes and Cipher Compilation Section of the Signal Intelligence Service, but also to the significant contributions he made in the field under discussion.

HISTORIAN, AS-13
15 November 1948

THE HISTORY OF ARMY STRIP CIPHER DEVICES

Contents

CHAPTER		PAGE
I.	Introduction	1
II.	Cipher Device M-94	8
	A. General	8
	B. Invention by Thomas Jefferson	9
	C. Invention by Etienne Bazeries	11
	D. Invention by Parker Hitt	13
	E. Invention by Major J. C. Mauborgne	15
	F. Approval as Standard; Procurement	18
	G. Use	22
	H. Conclusions	26
III.	Parker Hitt's Flat Strip Cipher Device	28
IV.	Development Models M-136 and M-137	30
	A. General	30
	B. Cipher Device M-136	30
	C. Cipher Device M-137	31
V.	Cipher Device M-138	34
	A. General	34
	B. Cipher Device M-138-T1	35
	C. Cipher Device M-138-T2	36
	D. Cipher Device M-138-T3	37
	E. Cipher Device M-138-T1, M-138-T2, M-138-T3, Tested by the Signal Corps Board	38
	F. Cipher Device M-138-T4	40
	G. Navy-developed Model of Cipher Device M-138	44
	H. Procurement of Cipher Device M-138	44
	I. Rotary Alphabet Strip Cutter	47
VI.	Cipher Device M-138-A	49
	A. Proposal for Modification of Cipher Device M-138	49
	B. Original Procurement and Revision of Specifications	49

CHAPTER		PAGE
	C. Procurement of Additional Cipher Device M-138-A	52
	D. Cancelled Order for 4,873 Cipher Device M-138-A	55
	E. Patent	56
VII.	Overcoming the Aluminum Shortage	58
	A. Cipher Device CSP 845 (Plastic)	58
	B. Unsatisfactory Service of Plastic CSP 845	59
	C. SIGWOW0	61
	D. Cipher Device CSP 845 (Metal)	62
	E. Summary of Procurement Problems	63
	F. Storage and Disposal of Obsolete Strip Boards	64
	G. Status of Registry and Security Classification and Transfer of Responsibility for Storage and Issue of Strip Cipher Devices	65
VIII.	Distribution of Strip Systems	69
	A. General	69
	B. Strip Systems as Stand-By Means of Communication	70
	C. Strip Systems as Normal Means of Communication	72
IX.	Security of Strip Cipher Systems	75
	A. General	75
	B. Rearrangement, Replacement, and Supersession of Alphabet Strips	77
	C. Selection of Generatrix	82
	D. Message Length Limitation	84
	E. Channel Elimination	85
	F. Split Generatrix	89
	G. Change from Fixed to Variable Number of Channels Eliminated	92
	H. Change from Channel Elimination to Strip Elimination	96

CHAPTER		PAGE
X.	Unadopted Proposals for Modification of Cipher Device M-94, M-138, M-138-A	105
XI.	Issue of Strip Systems to Holders Outside the United States Army	110
	A. U. S. Government Non-Military Organizations	110
	B. Foreign Governments	112

LIST OF FIGURES

FIGURE		OPPOSITE PAGE
1	The Family Tree of Army Strip Cipher Devices	8
2	The Hitt Alphabets	15
3	The Mauborgne Alphabets	16
4	Two Lines Enciphered on the Same Generatrix	75
5	Sample Key Table (1939 - 1942).....	80
6	Numerical Keys	81
7	Channel Elimination Numbers (Fixed).....	87
8	Channel Elimination Numbers (Variable)..	95

~~SECRET~~

LIST OF TABS

	TAB
Thomas Jefferson's own description of his "Wheel Cipher"	1
Parker Hitt's sketch of his Disk Device	2
Parker Hitt's Flat Strip Cipher Device (front view).....	3
Parker Hitt's Flat Strip Cipher Device (reverse side)...	4
Cipher and plain text of messages sent in 1918 to Riverbank Laboratories and to Cipher Bureau (MI-8) for cryptanalysis	5
U. S. Army Specification No. 72-26 for Cipher Device M-94, 20 May 1921	6
Cipher Device M-94, description and photograph	7
Cipher Device M-94, description continued and photograph of the device partly dismantled	8
Cipher Device M-136, description and photograph	9
Cipher Device M-136, description continued and photograph of the device partly dismantled	10
M-136 Alphabet Disk, description and photograph of the dismantled disk	11
Cipher Device M-137, description and photograph.....	12
Cipher Device M-137, description and photograph showing different position of parts with lever pulled down.	13
Cipher Device M-138-T1, photograph showing wooden lid closed	14
Cipher Device M-138-T1, photograph showing wooden lid open	15
Cipher Device M-138-T1, description and photograph of operating surface	16
Cipher Device M-138-T3, description and photograph.....	17
Cipher Device M-138-T3, description and photograph of operating surface	18

008

~~SECRET~~

	TAB
Cipher Device M-138-T4, description, photograph and method of operation	19
Signal Corps Board Case No. 193, 20 April 1934	20
Signal Corps Board Case No. 199, 7 June 1934	21
Cipher Device M-138, description and photograph	22
Cipher Device M-138, method of operation and photograph	23
Rotary Cutting Machine, draft specifications	24
Cipher Device M-138-A, photograph showing the lid closed	25
Cipher Device M-138-A, description, photograph showing operating surface, and method of operation	26
Cipher Device M-138-A (Wood), description, photograph, and method of operation	27
U.S. Army Specification No. 71-715-B, 7 April 1938	28
Cipher Device CSP 845 (Plastic), photograph showing lid closed	29
Cipher Device CSP 845 (Plastic), description and photograph showing operating surface	30
Cipher Device CSP 845 (Aluminum), photograph showing lid closed	31
Cipher Device CSP 845 (Aluminum), description and photograph showing operating surface	32
Procurement chart of Cipher Devices M-138, M-138-A, CSP 845 (Plastic) CSP 845 (Metal), and SIGWOB	33
Procurement of Strip Cipher Devices, Chronological outline	34
Removal of Classification and Registry Cipher Device CSP 845 and Similar Devices, Transmittal Sheet, 16 Nov 1944	35
Distribution of Cipher Devices M-138 and M-138-A, and number authorized on hand 9 September 1939	36
System 1501 - Number of copies distributed	37

	TAB
Cryptonet Distribution during World War II	38
Major Changes in the use of Strip Cipher Device	39
Channel Elimination and Split Generatrix, Chronology of change relating to	40
File References, Specifications, Nomenclature, Operating Instructions and Security Reports	41
Cryptographic Assistance Furnished Outside Agencies by the Army Security Agency	42
Report of Contacts Outside Security Division	43
Issue of Combined Cryptographic Systems to Allied Forces other than U. S. - British	44
Request from Costa Rica for Cryptosystem	45
Cryptographic Material for French Troops	46
Cryptographic Material for Italian Troops	47
Cryptographic Material for Philippine Army	48
Cryptographic Systems for Russian Armed Forces	49
Policy - Furnishing U. S. Army Cryptographic Systems to Russia	50

THE HISTORY OF ARMY STRIP CIPHER DEVICES

Strip cipher systems, both prior to and during World War II, played an important role in classified communications. Before and at the very beginning of the war a great deal of reliance was placed upon strip systems because the Armed Forces had not yet accomplished extensive distribution of cipher machines. Although strip cipher systems are admittedly inferior to the speedy cipher machines, which in part replaced them, they did their required job well. Nor were they outmoded when just after the beginning of World War II, cipher machines came into general use as the primary means of secret communication. Strip cipher systems remained tremendously important in two cases: (1) for use as a "stand-by" system in the event the cipher machine system should for any reason become inoperative; (2) for use in classified communications by holders not authorized high-grade machine systems.[1]

CHAPTER I. INTRODUCTION.

This history records the development of Army strip cipher devices and of the cylindrical cipher device from

---

1. For an extended discussion of the use and importance of strip cipher systems, see Chapter VIII, Pages 69-74.

which they evolved. Army strip cipher devices are channeled, flat boards, the channels of which hold sliding alphabet strips. The cylindrical device, which came into existence many years before the flat form, is composed of a central shaft on which is mounted a number of revolving disks containing alphabets on their peripheries. The cryptographic principles of the two types of devices are identical, since each provides encipherment by means of a number of different, sliding, mixed alphabets. In order that the reader may have a better understanding of the discussion which follows, it is necessary to present here a brief description of encipherment by means of each of these basic types of devices.

The alphabet disks of the cylindrical type can be removed from the central shaft and replaced in any given prearranged order.[2] After the disks are mounted on the shaft in the order agreed upon, the plain text of the message to be enciphered is aligned across the device in a horizontal line by revolving the disks one by one. The cipher text is chosen at random from the horizontal lines of letters resulting from this plain-text alignment. Succeeding lines of plain text are enciphered in the same

2. For pictures of a disk-type device, see the photographs of Cipher Device, type M-94, Tabs 7 and 8.

manner until the entire message has been converted into cipher text. Decipherment is performed by a reversal of the procedure, that is, the cipher text is aligned across the device and the resulting plain text can be found by examining the other horizontal lines of letters thus formed, only one of which will "read".

Flat Army strip cipher devices have their mixed alphabets on paper strips inserted in channels instead of on disks mounted on a shaft.[3] The difference between the two types is purely mechanical, since ordinary sliding strips bearing repeated alphabets produce the same results as single alphabets mounted upon wheels. For an example of a flat strip device, containing channels, see photograph of Cipher Device, type M-138-A, Tab 26. In general, to encipher a message using the flat type, the letters of the plain text are aligned in a vertical column at the edge of the device. Another vertical column, which results from the plain-text alignment, is chosen to serve as the cipher text. Succeeding lines of plain text are enciphered in the same manner until the entire message has been converted into cipher text. Decipherment is performed by a reversal of the procedure.

---

3. See Tabs 9 and 26.

The cryptographic strength of the disk or strip cipher lies in the variable factors which it provides, namely, encipherment by a number of different, sliding, mixed alphabets and a possibility of 25 different letters for each letter of plain text. The cryptographic weakness of the strip or disk cipher is the constancy of the interval (p. 75) between the letters of any one plain-text alignment and the letters of its cipher text generatrix (p. 75); it is this inherent characteristic which serves as the wedge for all cryptanalytic recovery of this type of system. All security improvements of the device itself and of methods of using it have been designed to prevent cryptanalytic establishment of this constant factor.

The first device of either type standardized by the Army was the cylindrical Cipher Device M-94 (Tabs 7, 8) which was independently invented by four different persons over a period of years. It was officially adopted in 1921 and used until 1943, when it was declared obsolete.

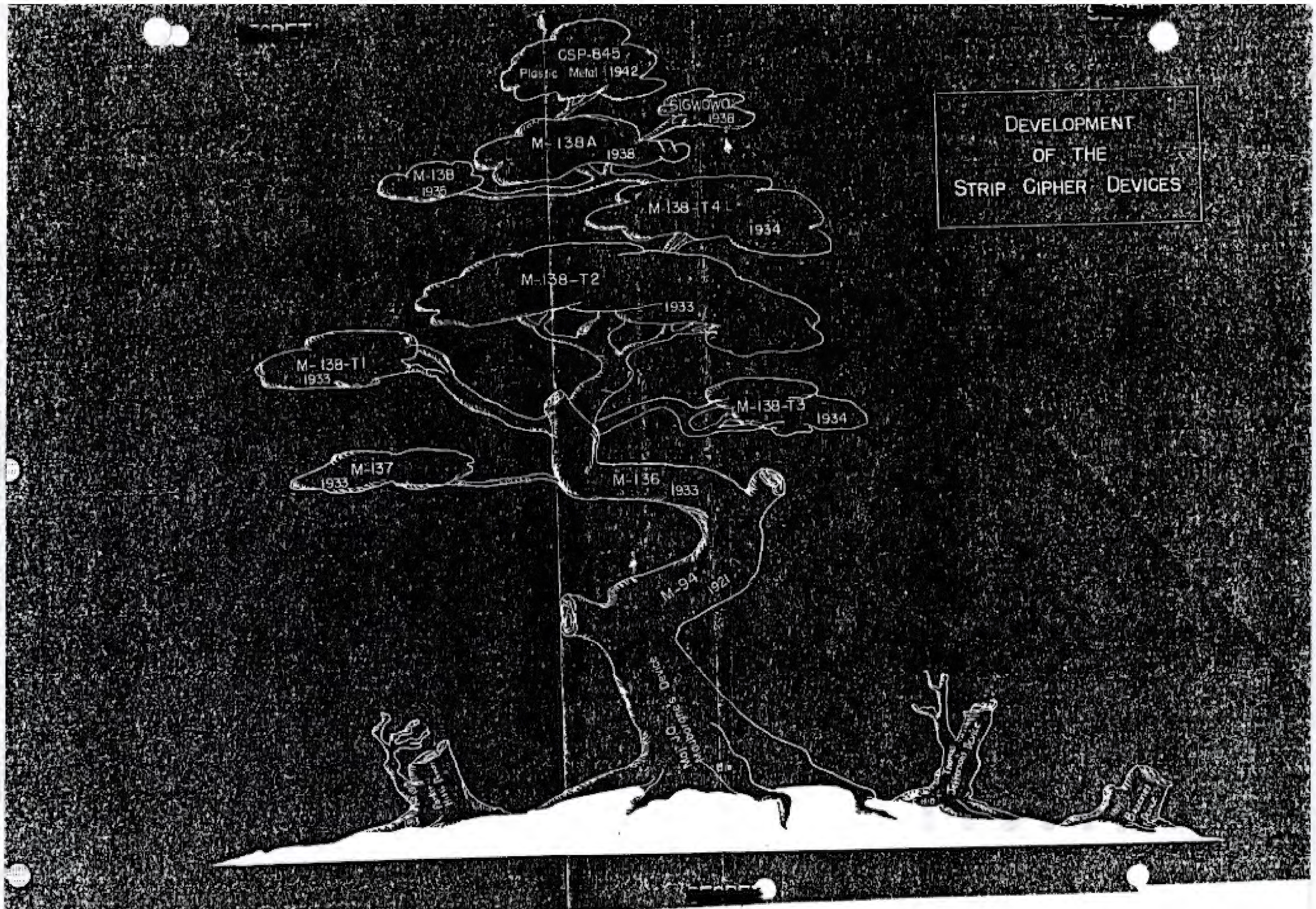
The first flat strip cipher device which was standardized for use by the Army was Cipher Device M-138 (Tabs 22, 23), officially adopted on 9 July 1934. This date announced the official recognition of the flat form of the strip device as valuable to cryptographic communications. However, even before 1921, the year in which Cipher Device M-94

was adopted, a flat strip cipher device in elementary form had been conceived by Parker Hitt (Tabs 3, 4). Many other development models were built by the Armed Services before the final Army form was adopted in 1934. The discussion, which follows, of these intervening models is simple if the central issue in their development is kept in mind: All Army experimentation with different mechanical forms of the cipher devices was directed toward the goal of providing an easy method of changing the alphabets used. Cipher Device M-94 did not provide this feature since its alphabets could be replaced only by manufacturing new disks. Planning and building a device which would easily allow this important feature and still work smoothly proved to be no little problem. The round Cipher Device M-136 (Tabs 9, 10) and the Navy-developed Cipher Device M-137 (Tabs 12, 13) were both unsuccessful attempts. Cipher Device M-138-T1, M-138-T2, M-138-T3, and M-138-T4 (Tabs 14 through 19) were models constructed, with certain differences, for the specific purpose of deciding which was mechanically more practical for allowing the change of alphabets. Finally, a Navy development, based on the Army-evolved Cipher Device M-138-T4, was adopted as standard, but this did not work properly when put into service. Therefore, new experimentation began which resulted in the excellent Cipher Device M-138-A (Tabs 25, 26),

and its initial procurement in the late 1930's. The only cryptographic change which this new device offered was the addition of 5 channels, making Cipher Device M-138-A a 30-channel device instead of a 25-channel device as was Cipher Device M-138.

Since Cipher Device M-138-A worked so well, it may seem strange that the Army should use three other models during World War II. There is only one reason for the use of the other three models. Cipher Device M-138-A was made of scarce aluminum. It was necessary therefore to find a substitute material to finish procurement of the number required by the Army's using forces. No suitable substitute material was ever found in spite of the fact that two other models were put into service. A wooden device of Honduras mahogany, called Cipher Device M-138-A (SIGWOWO) (Tab 27) was used by the Army but proved unsatisfactory because of warping in certain climates. The plastic CSP 845 (Tabs 29, 30), purchased in quantity from the Navy, was also tried but was unsatisfactory for the same reason. When aluminum finally became available in September 1943, aluminum Cipher Device CSP 845's (Tabs 31, 32) were ordered from the Navy because this course was, at the time, more expedient than renegotiating with the manufacturer for aluminum Cipher Device M-138-A's. The development, procurement, and

special problems concerning each of these devices is presented in detail under appropriate headings on pages 8 through 68; distribution and use of strip cipher systems is discussed on pages 69 through 74; and security improvements, which are extensive, are discussed on pages 75 through 104.


DEVELOPMENT
OF THE
STRIP CIPHER DEVICES
CSP-845
Plastic Metal 1942
SIGWOWO
1938
M-138A
1938
M-138
1935
M-138-T4
1934
M-138-T2
1933
M-138-T1
1933
M-138-T3
1934
M-137
1933
M-136
1933
M-94
1921
Not JO Wheelwright's Device

CHAPTER II. CIPHER DEVICE M-94

A. General

The Cipher Device M-94 operates on what is known as the revolving wheel principle. This is one of many of the various ways in which polyalphabets may be used in cryptography. In this case a number of different alphabets are used one after the other in a definite sequence, each alphabet encrypting one letter of plain text. If there are more letters of text than there are alphabets the same sequence of the alphabets is repeated until all the letters of the plain text have been encrypted. If the cipher text is divided into lengths equal to the number of alphabets used, it will be found that within each of these sets there is always the same interval between the plain and cipher components.

The insecurity of the system lies in the use of known alphabets which permits construction of Synoptic Tables. By use of these tables, and a known or suspected word or words in the text, the order of arrangement of the alphabets can be found. With the sequence of alphabets recovered, messages can then be decrypted easily. /See Chapter IX/

Several devices using the revolving wheel principle were conceived independently by different persons at various

periods. Four inventors are on record, namely, Thomas Jefferson; Commandant Etienne Bazeries of the French Army; Captain Parker Hitt, USA; and Major General (then Major) Joseph O. Mauborgne, USA. Thomas Jefferson's work was unknown to the other three men. Captain Hitt and General Mauborgne may possibly have known of Commandant Bazeries' work, though it is believed they were not aware of his invention. General Mauborgne did know of Captain Hitt's invention--or at least of the alphabets he used.

B. Invention by Thomas Jefferson

The first inventor, Thomas Jefferson, conceived a device which he called the "Wheel Cypher" and which very closely resembled the twentieth century Army Cipher Device, type M-94. The Cipher Device M-94, however, was invented and manufactured without knowledge of the existence of Jefferson's conception.[1]

---

1. Wm. F. Friedman, who in 1922 was Signal Corps Cryptanalyst and is now Director of Communications Research, Army Security Agency, states: "...when, in 1922, my friend Professor John Manly brought me a photostatic copy of the foregoing, in Jefferson's own handwriting, with all the corrections Jefferson made as he was describing his invention, I was much startled. For here was another beautiful example of the adage in cryptography that 'there is nothing new under the Sun'." Friedman, William F., "Edgar Allan Poe, Cryptographer," Signal Corps Bulletin, 98, (Oct.-Dec., 1937), reprinted in Articles on Cryptography and Cryptanalysis, prepared under the direction of the Chief Signal Officer, 1942.

To show the amazing similarity, Jefferson's own description is quoted below:[2]

> Turn a cylinder of white wood of about 2 in.diam. and 6 or 8 in. long. Bore through it's center a hole sufficient to receive an iron spindle or axis of 1/8 or 1/4 in diam. Divide the periphery into 26 equal parts (for the 26 letters of the alphabet) and with a sharp point draw parallel lines through all points of division from one end to the other of the cylinder and trace those lines with ink to make them plain. Then cut the cylinder crosswise into pieces of about 1/6 of an inch thick. They will resemble backgammon men with plane sides. Number each one of them as they are cut off, on one side, that they may be arrangeable in any order you please. On the periphery of each and between the black lines put all the letters of the alphabet, not in their established order, but jumbled and without order so that no two shall be alike, now string them in their numerical order on an iron axis, one end of which has a head and the other a nut and screw, the use of which is to hold them firm in any given position when you choose it. They are now ready for use, your correspondent having a similar cylinder similarly arranged.
>
> Suppose I have to cypher (these words) this phrase 'Your favor of the 22d is received.'
>
> | | |
> |---|---|
> | turn the 1st wheel till the letter | y. presents itself |
> | turn the 2d and place it', | o. by the side of the y. of the 1st |
> | turn the 3d and place it', | u. by the side of the o. of the 2d |
> | turn the 4th and place it', | r. by the side of the u. of the 3d |
> | turn the 5th and place it', | f.by the side of the r. of the 4th |
> | turn the 6th and place it', | a. by the side of the f.of the 5th |

2. A photostatic copy of the description in Thomas Jefferson's own handwriting is given in Tab 1. The original is in the Library of Congress, Jefferson Papers, Vol. 232, Item 41575. A reprint of the photostat is also contained in the article referred to in footnote 1.

and so on till I have got all the words of the phrase arranged in one line. Fix them with the screw. You will observe that the cylinder then presents 25. other lines, not in any regular series, but jumbled and without order or meaning. Copy any one of them in the letter to your correspondent. When he receives it, he takes his cylinder and arranges the wheels so as to present the same jumbled letters in the same order in (a) one line. He then fixes them with his screw and examines the other 25. lines and finds one of them presenting him these words 'Your favor of the 22d is received.' which he writes down. As the other will be jumbled and have no meaning he cannot mistake the true one intended. So proceed with every other portion of your letter....

C. Invention by Etienne Bazeries

In 1891, Commandant Etienne Bazeries, a noted French cipher expert, independently invented the same type of device.[3] His own description of the device is quoted:[4]

The apparatus consists of the following parts:

1. A cylindrical body, terminated at one extremity by a disk permanently fixed to the cylinder and bearing an indicator in the shape of a forked finger; at the other extremity by a milled disk, which screws onto the cylinder.

2. Twenty alphabets, each of twenty-five letters (Latin Script) in the form of rings which encircle the cylinder, the sequence of each alphabet being different from that in all the other alphabets. Each one bears a number on one side.

---

3. "A Multiplex Alphabet System," Several Machine Ciphers and Methods for their Solution, Publication No. 20, Riverbank Laboratories, (1918), p. 37.

4. This description, found in pages 250-261 of Bazeries book Les Chiffres Secrets Devoiles, Paris, 1901, was taken from Riverbank Laboratories Publication No.20 (1918).

3. A stop-pin, the head of which can be screwed into the fixed disk, and the stem of which, partially sunk into a groove running longitudinally on the cylinder, fits into notches on the inner side of the alphabet-rings, which notches correspond in position with the letters on the outer side.

The Key.--This is secured from the order in which the alphabet rings are placed on the cylinder. This order is derived from a word which is repeated until there is a total of twenty letters. To transcribe this word into numbers, a figure 1 is written beneath the letter which comes first in the normal alphabet; if it is repeated the second time it becomes number 2, a third time, number 3, etc. Then the letter which comes next in the normal alphabet is numbered in sequence, etc., until all the letters have been numbered.

* * * * * * * *

Setting the apparatus according to the key, that is, arranging the various alphabet rings in accordance with the succession of numbers given by this numerical key, the successive rings are so adjusted in relation to each other as to spell out in the line indicated by the forked finger the first twenty letters of the plain text. The successive rings are fixed one after the other during the process of pushing the stop-pin forward and thus through each ring as it comes into position. The cipher line is one single line taken from among the other horizontal lines. This operation is repeated for the next twenty letters and so on until the entire message has been enciphered. The process of decipherment is simply the reverse of the process of encipherment. The first series of twenty cipher letters being brought on the line opposite the indicator, the successive horizontal lines are inspected and the line containing the plain text will be found immediately because it will be the only one which presents an assemblage of letters forming intelligible words.

* * * * * * * *

The cylindrical cryptograph inaugurates a new method in cryptography. The principle is the following: the simultaneous employment of a multiplicity of alphabets for the encipherment of one and the same dispatch.

> The apparatus does not need to be kept in concealment, since it does not betray the secret, on condition of course that it be taken apart. The operation of it is simple and rapid and the indecipherability absolute. There is nothing kept secret except the key-word."

It "may be assumed----with a high degree of probability that Bazeries had no knowledge of Jefferson's cylinder."[5] However, the French inventor added to Jefferson's method the later-adopted Army procedure for arranging the disks according to a numerical sequence derived from a key word.

D. Invention by Parker Hitt

The next inventor was Captain Parker Hitt, now Colonel, United States Army, retired, then Captain of the 19th Infantry. In 1913, Captain Hitt was an instructor at the Army Signal School, Ft. Leavenworth, Kansas. Although the course in cryptography was very elementary, "the necessity for enciphering radio messages was stressed. The only equipment for this purpose was the old Signal Corps Cipher Disk."[6] During the field exercises of the spring of 1913, some of the students solved enciphered "enemy" radio messages almost as soon as they were intercepted. This easy solution by the students caused Captain Hitt to ponder the

---

5. Ibid., p. 183.

6. Ltr from Parker Hitt, to Wm. F. Friedman; 9 Aug 47; AS-80A File: "Cipher Device M-94."

possibility of a "safer, simpler system for field use."[6] During the summer of 1913 he conceived a device which he himself described as follows:[6] (The description should be read in connection with the sketch he drew to supplement his explanation. Tab 2)

During the summer of 1913 I figured out one like this...

a. Ten cipher disks, each with a regular alphabet and an individual mixed alphabet, the alphabets appearing on the rim. The disks had a central hole and were numbered so that they could be placed on a central spindle in any agreed order.

b. The central spindle had a reading strip, fixed, through the windows of which the plain text alphabets of the ten disks could be read. A movable reading strip pivoted at each end of the spindle had windows to read the mixed alphabets only. The position of the movable strip was variable and was shown by an indicator on one end of the spindle.

c. To use, each of the ten cipher disks was to be set according to a key, (A to S, A to I, A to G, etc.) and then they were placed on the spindle in an agreed order and the movable reading strip was set at an agreed line number. The plain text being set in the windows of the mixed strip, the cipher to be sent was read in the windows of the movable strip. For receiving, the process was reversed.

To make his idea a reality, Captain Hitt had some cylinders of applewood turned and then had a hole bored through the centers. Next he cut the cylinders into disks and glued typed paper strips on their peripheries. It can readily be seen that although the above described device, with its ten plain alphabets, ten cipher alphabets, and two reading strips with

windows, resembled Cipher Device M-94, it was far from an exact replica. The last step of accomplishment, however, occurred accidentally. Parker Hitt described the final evolution of his idea for the cylindrical device as follows:[7]

> One day during the summer of 1913 I went into the lab shop to work...and picked up a rod on which I had strung ten mixed alphabet disks for safe keeping the day before. By pure accident, one line of the first two disks spelled TH and the idea came to me to discard the plain text disks and the reading strips and to set plain text on <u>any</u> line of the mixed alphabet disks and to send <u>any other</u> line as the cipher message. This would involve only an agreement between correspondents as to the order in which the mixed alphabet disks were placed on the spindle....

He never constructed a working model of his final conception of the disk device but, according to Hitt's own words, "the idea of the flat form using double length paper strips was a perfectly natural evolution...."[8] Since he preferred the flat form (Tabs 3,4) he abandoned his idea of the disk device. The evolution of his flat strip device is further described on page 28.

E. Invention by Major J. O. Mauborgne

The inventor whose disk cipher device was adopted by the War Department was Major General (then Major) J. O. Mauborgne, Chief, Engineering and Research Division, Office

---

7. Ibid.
8. Ibid.

Figures 2

THE HITT ALPHABETS

A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
E	E	E	E	N	E	E	E	E	V	E	E	E	E	M	E	E	E	E	K	E	E	E	E	H
I	I	I	R	R	I	I	I	X	X	I	I	I	Z	Z	I	I	I	P	F	I	I	I	R	R
O	O	S	S	S	O	O	Z	Z	Z	O	O	J	J	J	O	O	W	U	W	O	O	S	S	S
U	T	T	T	T	U	J	J	J	J	U	K	K	K	K	U	Y	Y	Y	Y	G	T	T	T	T
H	H	H	H	K	K	K	K	K	Q	Q	Q	Q	Q	L	L	L	L	L	H	H	H	H	H	H
E	N	N	N	C	Q	Q	Q	Q	Q	V	V	V	V	V	M	M	M	K	Z	N	N	N	E	J
R	R	R	D	D	V	V	V	V	C	X	X	X	X	N	P	P	P	J	J	R	R	R	K	K
S	S	F	F	F	X	X	X	D	D	Z	Z	Z	R	R	W	W	K	K	K	S	S	Q	Q	Q
T	G	G	G	G	Z	Z	F	F	F	J	J	S	S	S	Y	Q	Q	Q	Q	T	V	V	V	V
B	B	B	B	B	J	G	G	G	G	K	T	T	T	T	V	V	V	V	V	X	X	X	X	X
C	C	C	C	M	B	B	B	B	B	H	H	H	H	H	X	X	X	X	X	Z	Z	Z	Z	Z
D	D	D	P	P	C	C	C	C	N	N	N	N	N	M	Z	Z	Z	Z	N	J	J	J	J	C
F	F	W	W	W	D	D	D	R	R	R	R	R	F	P	J	J	J	R	R	K	K	K	D	D
G	Y	Y	Y	Y	F	F	S	S	S	S	S	W	W	W	K	K	S	S	S	Q	Q	F	F	F
L	L	L	L	L	G	T	T	T	T	T	Y	Y	Y	Y	Q	T	T	T	T	V	G	G	G	G
M	M	M	M	Q	H	H	H	H	H	L	L	L	L	L	H	H	H	H	H	B	B	B	B	B
P	P	P	V	V	N	N	N	N	M	M	M	M	M	C	N	N	N	N	C	C	C	C	C	M
W	W	X	X	X	R	R	R	P	P	P	P	P	D	D	R	R	R	D	D	D	D	D	P	P
Y	Z	Z	Z	Z	S	S	W	W	W	W	W	F	F	F	S	S	F	F	F	F	F	W	W	W
J	J	J	J	J	T	Y	Y	Y	Y	Y	G	G	G	G	T	G	G	G	G	G	Y	Y	Y	Y
K	K	K	K	K	L	L	L	L	L	B	B	B	B	B	B	B	B	B	B	L	L	L	L	L
Q	Q	Q	Q	E	M	M	M	M	E	C	C	C	C	E	C	C	C	C	E	M	M	M	M	E
V	V	V	I	I	P	P	P	I	I	D	D	D	I	I	D	D	D	I	I	P	P	P	I	I
X	X	O	O	O	W	W	O	O	O	F	F	O	O	O	F	F	O	O	O	W	W	O	O	O
Z	U	U	U	U	Y	U	U	U	U	G	U	U	U	U	G	U	U	U	U	Y	U	U	U	U

of the Chief Signal Officer, afterwards Chief Signal Officer. Sometime between September 1916 and August 1917 while Major Mauborgne was Assistant Commandant of the Signal School at Fort Leavenworth, Kansas, he examined the Hitt alphabets[9] (See Fig. 2 opposite page 15) and decided that, because the letters were not thoroughly scrambled, the messages produced were too easily deciphered. This decision instigated his determination to make a 25-disk device--"each disk to have on it 26 letters of the alphabet, non-repetitive on any disk and as far as possible so arranged that the fewest number of repetitions of pairs of letters....would occur."[10] The alphabets which Major Mauborgne produced (See Fig. 3 on opposite page) were the ones adopted.[11] According to his own description he composed them as follows:[10]

---

9. The cipher system invented by Parker Hitt, including the Hitt alphabets, was referred to by Riverbank Laboratories as the Star Cipher. "A Multiplex Alphabet System," Publication No. 20, Riverbank Laboratories (1918) p.34.

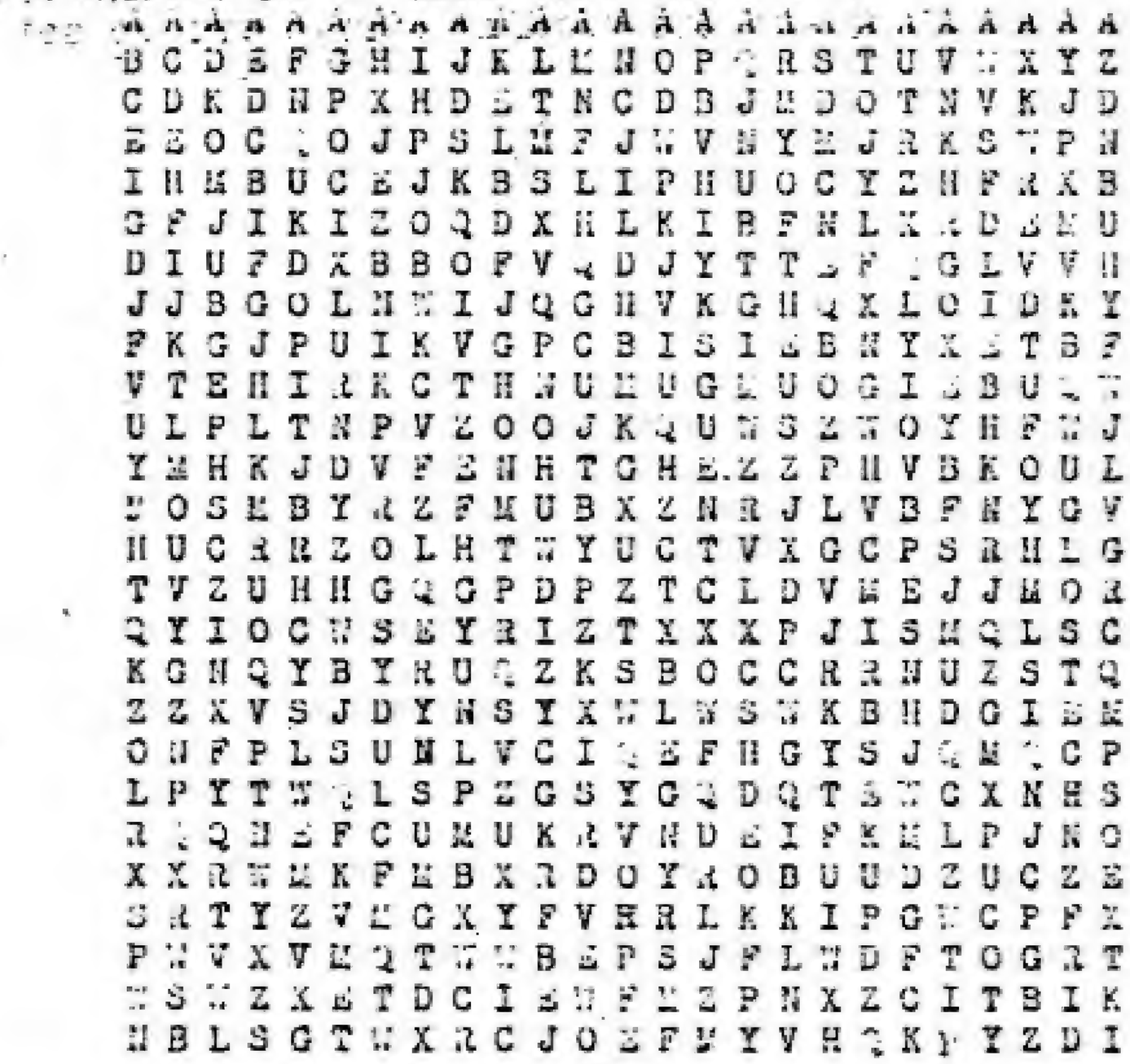
10. Ltr to Wm. F. Friedman from J. O. Mauborgne; 16 Aug 47; AS-301 File: Cipher Device M-94.

11. Cipher Device M-94 bears the brand of the Army, the R disk (the one designated as R-17, on which R follows A) having its letters arranged so as to spell ARMY OF THE U. S. Another disk, the Y disk (the one designated as Y-24, on which Y follows A), has its letters arranged so as to spell out the word FRIDAY. See Figure 3.

Figure 3

THE HAUDORCHS ALPHABETS

(Alphabets of Cipher Device M-94)



. . . I made a table of pairs from which I scratched out pairs already used as I proceeded until I had used them all up. Due consideration had to be given to the fact that the 26th letter for a particular disc had to tie on as a pair with the "A" or initial letter of each disc. Naturally there would be no pairs of similar letters, AA, BB or others.

My table looked like this sample:

AB	BA	CA	DA	EA	FA	GA	HA	IA	JA	KA	LA	etc.
AC	BC	CB	DB	EB	FB	GB	HB	IB	JB	KB	LB	etc.
AD	BD	CD	DC	EC	FC	GC	HC	IC	JC	KC	LC	etc.
AE	BE	CE	DE	ED	FD	GD	HD	ID	JD	KD	LD	etc.
AF	BF	CF	DF	EF	FE	GE	HE	IE	JE	KE	LE	etc.
AG	BG	CG	DG	EG	FG	GF	HF	IF	JF	KF	LF	etc.
*	*	*	*	*	*	*	*	*	*	*	*	etc.
*	*	*	*	*	*	*	*	*	*	*	*	etc.
AZ	BZ	CZ	DZ	EZ	FZ	GZ	HZ	IZ	JZ	KZ	LZ	etc.

When I had finished the laborious task of making the pairs all fit with the least repetitions, I found that I had to use the three pairs DE YA and UB twice instead of only once, so my first assignment of a name to the cipher was the name of the pairs "DEYAUB" . . .

Major Mauborgne had two copies of his cipher device constructed in early 1917 by M. S. E. Dusenbury in the shop of the Army Signal School at Fort Leavenworth, Kansas. These two devices were identical except that one was made of red fiber and the other of hard rubber. In early 1918, by which time Major Mauborgne was in charge of the Engineering and Research Division, Office of the Chief Signal Officer, he had a series of messages enciphered with his own alphabets. The beginnings of these 25 messages were sent, on 23 April 1918, to both the Riverbank Laboratories, Geneva, Illinois and to the Cipher Bureau (MI-8) for cryptanalysis. They were never solved.

Because of the high resistance to solution shown in this test,[12] Major Mauborgne's device and his special alphabets (opposite p. 16) became the Army Cipher Device, type M-94 (Tabs 7, 8). Some 20 years later, in 1941 after General Mauborgne had retired, when the clear text of the messages used for the test came to light, the reason for the failure became apparent. This clear text was English but the words employed were so seldom used and so little known as to be unrecognizable. Photostatic copies of both the plain and cipher text of the beginnings of the 25 messages sent to Riverbank and to MI-8, are shown in Tab 5.

F. Approval as Standard; Procurement

Three years elapsed after the test messages were sent to MI-8 and to Riverbank Laboratories and before the disk device was approved by the Signal Corps Technical Committee. At meeting No. 8[13] of the Signal Corps Technical Committee,

---

12. This test consisted of the beginnings of 25 messages, each 25 letters long. After quite a bit of work had been done and no results had been obtained, a request was made by Riverbank Laboratories for a word of clear text which actually occurred in one of the messages. The words ARE YOU were given, and these were tried in every possible position. When the results were examined, no further clear text, nor any likely combinations of letters which seemed plausible as parts of words, were noted.

13. All information on Signal Corps Technical Committee meetings was obtained from the files of minutes of SCTC meetings, Engineering and Technical Service, OCSigO, The Pentagon.

22 March 1921, a list of all signal equipment appearing in various War Department circulars of basic allowance was approved as standard; the list included Cipher Device M-94 (Tabs 7, 8). This same list was approved by the Secretary of War on 16 April 1921.[14] At meeting No. 12[13] held on 15 June 1921, Specification No. 72-26[15] (Tab 6) for Cipher Device M-94 was approved by members of the Technical Committee and concurred in by representatives of the using services present.

The initial order for Cipher Device M-94 in quantity was placed with the Doehler Die Casting Company, Court, Ninth, and Huntington Streets, Brooklyn, New York,

---

14. The list of signal equipment here mentioned was compiled in accordance with a directive of the Secretary of War. Definite channels for standardization were evidently not clearly defined in 1920. However, a decisive beginning was made as evidenced by the following: The Secretary of War directive (to AG, from Ass't Chief of Staff, 17 May 1920) stated, "There is some confusion in the minds of the using service as to exact standard or approved models, and it is desired to establish standards in all articles prescribed in basic tables for issue to the Army." A directive to effect this action was sent by the AG not only to the OCSigO but also to other services. OCSigO prepared the list of Signal Equipment (which included Cipher Device M-94) as directed and sent it to The Adjutant General for approval of the Secretary of War. The Secretary of War directed OCSigO to first obtain the approval of the Signal Corps Technical Committee. This approval was obtained at SCTC meeting No. 8. National Archives File 311.5.

15. For Specification 72-26-A, see footnote 17 p. 23.

in 1921.[16] This company was selected from several which submitted bids and samples for the manufacture of the aluminum device. Actual design of the device was contributed by Major L.M. Evans, Electrical Engineering Laboratory, Research and Development Division, and representatives of the Doehler Company.

On 21 March 1928 an additional order for Cipher Device M-94[17] was placed with the Reeve Electrical Company, Brooklyn, New York. The specific increase in distribution responsible for this order is unknown. The Reeve Electrical Company supplied 546 cipher devices under Order No. W-457-sc-726, 100 of which were furnished for Coast Guard use with special discs in accordance with Order No. 2151-Ny-29. The contractor also supplied 548 of the cipher devices under Order W-227-sc-22, all of which were

16. The meager information on procurement given here was gleaned from incidental reference to Cipher Device M-94 in files of letters concerning rejected amateur cipher systems filed in the National Archives. A small amount of additional information on procurement was found in file 461 (M-94) Cipher Device No. 1, 1921 thru (Obs.1945), WD Records Br., 219 N. Lee St., Alexandria, Va.

17. Specification used for this contract was Spec. No.72-26-A, approved at SCTC meeting No. 65 held 1 Mar 26. From files of SCTC Meeting Minutes, Engineering and Technical Services, OCSigO, The Pentagon.

~~SECRET~~

forwarded to Signal Depot, New Cumberland, Pennsylvania.[18]

Just how many of the Cipher Device M-94 were manufactured by the two companies is unknown. However, on 5 May 1921, a letter[19] signed by Major J. O. Mauborgne, Research and Development Division, OCSigO, stated that 5,000 were desired. Although 5,000 was the number desired, a memorandum[20] sent two months later, on 19 July 1921, requested that only 2,000 be secured. The discrepancy in these figures was due to an unexpected rise in price caused by a necessity for placing the contract with the Doehler Company instead of with the lowest bidder.[21]

---

18. Ltr from New York General Depot, sgnd Priner, Senior Inspector, S.S. & L., to Capt. G. L. Thompson, 30 Apr 30. File 461 (M-94) Cipher Device No. 1, 1921 thru (Obs.1945), WD Records Br., 219 N. Lee St., Alexandria, Va.

19. Ltr from Maj. J. O. Mauborgne, Electrical and Signal Engineering Sec., Research and Development Div., OCSigO, to Col. Hanson B. Black, Purchase Sec., Supply Div., OCSigO, 5 May 21. File: same as above.

20. Ltr from Maj. Alfred E. Larabee, Research and Development Div., OCSigO, to Supply Div., OCSigO, 19 Jul 21. File: same as above.

21. The lowest bidder was the Veeder Manufacturing Co. in Hartford, Conn., which failed to agree on the "eight hour clause" of the contract, thus preventing placement of the contract with that company. Ltr from Maj. J.O. Mauborgne, Electrical and Signal Engineering Sec., Research and Development Div., OCSigO, to Col. Hanson B. Black, Purchase Sec., Supply Div., OCSigO, 5 May 21. File: same as above.

~~SECRET~~

The figures quoted above (consisting of the 2,000 ordered from the Doehler Company in 1921 and the 1,094 ordered from the Reeve Company in 1928) give a total procurement of 3,094 devices. Eventually these procurement figures were increased until almost 10,000[22] Cipher Device M-94's were procured. No record has been discovered which tells how and when these additional devices were procured.

G. Use

Cipher Device M-94 was used extensively between World War I and World War II. In February 1922 an instructional pamphlet entitled "Instructions for Using Cipher Device M-94" was published by the Office of the Chief Signal Officer. It stated that "the cylindrical cipher device will be issued to all message centers. Its primary use, however, is by message centers within the Infantry regiment and supporting troops." In 1927 there was an almost simultaneous issuance of Cipher Device M-94 (Navy title:

---

22. Mr. Friedman verified the procurement figures given in the quotation below: "The above was completed in Sept 41 for 9432 and we have no record of any more of these devices as being on order." Routing and Work Sheet, Sub: Cipher Device M-94, Action 1, to Lt. M. M. Kilgo, Statistical Sec., Procurement Div., 14 Feb 42. File: same as above.

~~SECRET~~

CSP 488) by the War and Navy Department for joint communications. It was widely distributed; the simultaneous effective date for its joint use being 1 September 1927. Keywords could be arranged by agreement between interested parties. However, a universal emergency keyword, which was changed only infrequently, could be used in the absence of any previous agreement. In December 1929 and January 1930, military[23] and naval[24] attaches were added to the holder list for Cipher Device M-94 and for the universal emergency keyword. Approximately nine years later, in September 1939, units of the Coast Guard were added to the Army and Navy Commands holding the universal emergency keyword for Cipher Device M-94.[25]

Plans for discontinuing use of Cipher Device M-94 began with the service tests conducted on Converter M-209. These service tests resulted in a recommendation "by SIS in February 1941 to the Signal Corps Technical Committee that con-

---

23. Circular ltr No. 440 from Maj. W. H. Simpson, Executive Officer, G-2, to All Military Attaches, Sub: Signal Corps Cipher Device T. M-94, 3 Dec 29; AS-SCA File: Cipher Device M-94.

24. Ltr from Chief of Naval operations to All Naval Attaches, Sub: Secret Communication Between Naval and Military Attaches, 14 Jan 30; File: same as above.

25. CSP 493, "Instruction for Using Cylindrical Cipher Device," Change No. 19, 1 Sept 39; File: same as above.

~~SECRET~~

sideration be given to the adoption of the M-209 as standard equipment for issue as replacement for Cipher Device M-94 on the basis of issue recommended by the boards of the several branches."[26]

In the spring of 1942 Security Section personnel, Signal Security Agency, learned that Cipher Device M-94 was being used by the Ferrying Command for messages carrying the date and time of arrivals and departures of troop ships. Representative traffic was obtained and read cryptanalytically without difficulty.[27] This success in reading the messages "was reported to the Air Force on 28 March 1942, calling attention to the ease with which keys could be reconstructed when messages were carelessly handled, thus permitting the reading of all messages intercepted in the same key." On 4 April 1942 a memorandum from Signal Security Division recommended:

> .. that the use of Cipher Device M-94 by both freight and troop transports be discontinued at once due to lack of cryptographic security of the system involved. It has been found possible to recover the key of the device using a very few messages. It is felt that using this insecure system is worse than using no system at all as it gives the correspondents a false sense of

---

26. "Historical Survey of Strip Cipher Systems," Strips, I, p. 2; filed in Literal Systems Subsection, Analysis Section, AS-83.

27. Ibid., "It was previously known that the assembly of disks could be determined by means of synoptic tables, given a single message in which a word was known."

security.

In the latter part of 1942 Converter M-209 was issued to several units to replace the M-94 and thereafter to other units as fast as M-209's became available. The issue of Cipher Device M-94 to troop units or to Posts, Camps, and Stations was discontinued 16 April 1943. The M-94 was used by some units of the Air Force after it had been superseded by Converter M-209, and by Ground Forces in North Africa through 1943. There were not enough Converter M-209's at that time to supply all units. On 13 July 1943 Signal Security Division sent the following letter to the Commanding General, Army Air Force, Technical Services Division, Washington, D. C.:

> It is requested that the use of Cipher Device M-94 be discontinued by Air Force Units. The device is no longer considered to afford any cryptographic security. It is considered a hindrance rather than an aid to communications since it tends to give the originator of the message a false sense of security.[28]

On 3 May 1943, at Meeting No. 261,[29] the Signal Corps Technical Committee approved the recommendation of the Sub-committee on Reclassification to reclassify Cipher Device M-94 from Standard to Limited Standard. During the discus-

---

28. Ibid. p 4.

29. All information on SCTC meetings contained in this paragraph was obtained from the files of minutes of SCTC meetings, E&T Services, OCSigO, The Pentagon.

tion at the meeting Colonel E.J. Magee, Chairman, explained that a gradual replacement of Cipher Device M-94 by Converter M-209 was enticipated and that Cipher Device M-94 would be withdrawn from service as soon as enough Converter M-209's were available. On 9 August 1943, at Meeting No. 275, Cipher Device M-94 was declared obsolete[30] by the Signal Corps Technical Committee. There were on hand at that time sufficient Converter M-209's to complete the replacement.

H. Conclusions

It is very "easy for us to condemn old devices in the light of later knowledge, and the M-94 looks childishly simple to us now, but let nobody underestimate the good purpose that it did serve at a period when something better than the old Cipher Disk and Playfair was badly needed."[31] Major Mauborgne's faith in the security of the device was no doubt higher than warranted. Nevertheless if the test

---

30. The recommendation for this action came to the SCFC from Signal Security Branch through Equipment Coordination Branch and finally through the SCFC Subcommittee on Reclassification.

31. The ideas and quotations in this paragraph are from informal notes on the history of Cipher Device M-94 written by Wm. F. Friedman on 11 Sep 47. Mr. Friedman became Signal Corps Cryptanalyst on 1 Jan 21 and is now (1947) Director of Communications Research,ASA. The Playfair was at one time the official cipher of the British Army. The "informal notes" referred to are filed in AS-60A, File: Cipher Device M-94.

~~SECRET~~

messages sent to Riverbank Laboratories and MI-8 had been solved and his device rejected, it probably would have been "necessary to struggle along for another dozen or more years with nothing better than the old Army Disk[32] and the Playfair Cipher." Major Mauborgne's "known practical experience in cryptanalysis and his official position at the time in the Office of the Chief Signal Officer lent weight to his statements as to the security of, need for, and desirability of such a device."[33] Since the relatively small funds required to produce the devices were available, it was logical for the Signal Corps Technical Committee to give its approval. Its adoption facilitated cryptographic operations and started the trend towards the use of ciphers instead of codes.

---

32. The only Cipher Device known to American Expeditionary Force in 1917.

33. Informal notes on the history of Cipher Device M-94 by Mr. Wm. F. Friedman, 11 Sep 47.

~~SECRET~~

~~SECRET~~

CHAPTER III. PARKER HITT'S FLAT STRIP CIPHER DEVICE

The first strip cipher device, employing fixed or invariable sequences, was conceived and constructed in 1915 by Parker Hitt, then a Captain in the Infantry, later a Colonel in the Signal Corps. This flat device was an outgrowth of the idea for a cylindrical device[1] which he conceived in 1913 (p.13-15). This device was never used for military communication, but it is of historical significance in the fact that it was the first flat device employing the cryptographic principle originally invented by Thomas Jefferson. No flat strip device was adopted for Army communication until 1934 when Cipher Device M-138 was approved, although such devices had been used for cryptanalytic purposes for many years prior to that.

Captain Hitt built the flat model at the School of Musketry, Fort Sill, Oklahoma (Tab 3, 4). He and Mrs. Hitt used it for many years for their personal confidential correspondence.[2] The model took the form of a set of juxtaposed

---

1. In the fall of 1943, while checking over old chests preparatory to moving, Col. Hitt found his original model of the flat strip device and, on 9 Sep 43, took pictures of it for the record. Information from Ltr from Parker Hitt To: Mr. Friedman, 9 Aug 47. AS-80A, Cipher Device M-138-A.

2. Ibid.

~~SECRET~~

sliding strips of wood[3] bearing the Hitt alphabet (Figure 2, p.15) on strips of paper.

Captain Hitt's device was once submitted to the War Department and rejected. In 1917 and 1918 when Mrs. Hitt was in charge of code and cipher work of the Southern Department, Military Intelligence Division, San Antonio, Texas, the courier mails to Mexico City were robbed on several occasions, necessitating that new enciphering sheets be furnished to all border stations. During the winter of 1917-18 Mrs. Hitt made a trip to Washington, taking along her husband's flat strip cipher device. She showed the model to Captain Herbert O. Yardley, who was then in charge of the Code and Cipher Section of Military Intelligence Division, and asked his permission to use it between San Antonio and Mexico City where the robberies had made code book communication unsafe. Yardley refused this permission, giving the reason that a new code book with an "unbreakable" enciphering system was about to be distributed; he also stated that there was no need for an emergency system.

---

3. Friedman, William F., "Edgar Allan Poe, Cryptographer," Signal Corps Bulletin, 98, (Oct-Dec, 1937), reprinted in Articles on Cryptography and Cryptanalysis, prepared under the direction of the Chief Signal Officer, 1942; p. 181.

~~SECRET~~

CHAPTER IV. DEVELOPMENT MODELS M-136 AND M-137

A. General

Late in 1933 plans were devised for an improved Army cipher device using the basic principle of Cipher Device M-94. The improvement desired was a means of substituting at will a completely new set of random alphabets. Attempts to provide this added security feature resulted in three new types of devices, namely, Cipher Device M-136, M-137, and M-138. The first two devices, which are discussed in this chapter, are of historical importance only. The third, Cipher Device M-138, has a development of its own which is discussed in CHAPTER V.

B. Cipher Device M-136

Cipher Device M-136 is a cylindrical device composed of aluminum alphabet disks mounted on a bakelite shaft and supported by a metal base (Tab 9). Paper alphabet strips are fastened on the peripheries of the disks by means of wire springs (Tab 11). Cipher Device M-136 was never used and no instructions for it were ever written. However, it may be assumed that enciphering a message would be performed in a manner similar to enciphering by means of Cipher Device M-94.

Mr. William F. Friedman furnished the design and drawing from which the disk-type experimental model, Cipher Device M-136, was made. At the request of War Plans and Training Division, the nomenclature Cipher Device type M-136 was assigned to this experimental device by Supply Division, Office of the Chief Signal Officer, on 15 June 1933. The National Electric Supply Company, 1330 New York Avenue, N. W., Washington, D. C. submitted a bid of $84.00 for the construction of one such device[1] from the drawings furnished by Mr. Friedman. When it was delivered for inspection, Mr. Friedman considered the device unsatisfactory because of the impracticability of mounting the strips properly and because the device itself was bulky and hard to use.

An attempt to align plain text on the device proved it was extremely difficult to run the removable rod (Tabs 9, 10) through the small holes in the disks without knocking the letters out of alignment. It was also impossible to see the generatrices underneath the disks because they were hidden by the metal base.

C. Cipher Device M-137

Cipher Device M-137 is mechanically the most complicated of the strip devices. It consists of a board supported at

---

1. Purchase Order No. SC-109335, P 37250; Procurement Authority No., SC 5413-P-13-1361-A-541-3.

a 45° angle by an aluminum frame. Paper alphabet strips move up and down the surface of the board by means of pulley wheels, a lever, and complicated coil springs which hold the strips together underneath the board (Tabs 12, 13).

The short-lived Cipher Device M-137, conceived in its special form by Lieutenant Smellow, Code and Signal Section, Navy Department, was developed exclusively within the Navy and was used by them for about three years.[2] Late in 1933 25 of these devices were presented by the Navy to War Plans and Training Division, Office of the Chief Signal Officer. It was considered for Army use very briefly and then only for joint communications in the event that the Navy kept it in service at shore stations.[3] The Army nomenclature (M-137) requested by War Plans and Training Division, was assigned by the Nomenclature Section, Office of the Chief Signal Officer, on 17 August 1933.[4] Nine days later, on 26 August 1933, the nomenclature assignment for Cipher Device

---

2. Information in this paragraph and the next, unless otherwise designated, was received by telephone from Mr. Friedman on 20 Jan 47.

3. Memo. for Maj. S. B. Akin from Wm. F. Friedman, 26 Jan 34. AS-80A File: Cipher Device M-137.

4. Information on nomenclature assignment for Cipher Device M-137 was provided by Nomenclature Section, OCSigO, The Pentagon.

M-138 was made; the nomenclature request designated the new device as "a modification of Cipher Device M-137."[5]

With the exception of about two devices, the Navy gift of 25 Cipher Device M-137's were returned. They proved unsatisfactory in naval service because of the mechanical imperfection of the coil spring arrangement. The coil springs were designed to perform the dual function of holding the ends of the alphabet strips together and of returning the alphabet strips to their original position. The springs became entangled in the bar attachment when the lever was operated. Also, the device was bulky, unwieldy, hard to manipulate, subject to expansion and contraction with the weather, and the paper strips were difficult to produce and to attach properly.

---

5. Memo. to Supply Division from Maj. S. B. Akin, 25 Aug 33. 1st Ind. To: WP&T Div., From: Supply Div., CCSigO, 26 Aug 33. AS-8CA File: Cipher Device M-136.

CHAPTER V. CIPHER DEVICE M-138

A. General

Cipher Device M-138 was the first flat strip device standardized and adopted for use.[1] Before standardization and procurement were effected, however, five experimental models were considered. The first four models were part of a definite authorized Army plan to perfect a model for production. The two devices, M-138-T1 and M-138-T2, were constructed under the direction of the Chief Signal Officer, and the third, M-138-T3, was obtained from the Navy. These three models were tested simultaneously by the Signal Corps Board for their recommendations on adoption. The board's conclusions resulted in the construction of a fourth model, Cipher Device M-138-T4, which was an improved version of the T2 model. With the intention to procure the T4 model, Cipher Device M-138 was officially adopted as standard in August 1934. However, before procurement was effected, the Navy, using the T4 model as a guide, built a fifth model which was believed to have a more satisfactory channel construction. This fifth model was procured as Cipher Device M-138 (Tab 22, 23).

---

1. For patent issue, see p.56.

B. Cipher Device M-138-T1

The first experimental model of Cipher Device M-138, eventually referred to as Cipher Device M-138-T1,[2] consisted of a heavy aluminum board with 25 channels milled into its surface and enclosed in a hinged wooden box with a leather handle (Tabs 14, 15, 16). The formal request for the new device was initiated by War Plans and Training Division on 1 September 1933,[3] and the construction was done by Signal Section of the New York General Depot in Brooklyn. Plans for construction of model 1 were formulated by the Signal Intelligence Section, War Plans and Training Division; however, details of manufacture were adjusted in accordance with improvements which the actual building of the model seemed to make more feasible. The finished product was shipped on 4 November 1933 by the Brooklyn Depot to the office

---

2. "For purposes of identification, it is requested that Register No. 1, Cipher Device, Type M-138, Model 3, S.C., U.S. Army . . . be in future referred to as "Cipher Device, type M-138-T3 . . . It is requested that Model No. 1 of Cipher Device, type M-138 be in future known as "Cipher Device, type M-138-T1" and the Model 2 be known as the "Cipher Device M-138-T2" . . . It is requested the Cipher Device, type M-138, which you are building based on the military characteristics as set up by the Signal Corps Board, be known as "Cipher Device, type M-138-T4." Ltr from Maj. Hugh Mitchell to OIC, Signal Corps Laboratories, Ft. Monmouth, N. J., 4 May 34; AS-80A File: Cipher Device M-138.

3. Memo from Maj. S.B. Akin to Supply Division, 1 Sep 33. AS-80A File: Cipher Device M-138.

of the Chief Signal Officer[4] approximately two months after the original request for the model was placed. The total cost of building the sample was $67.13.

C. Cipher Device M-138-T2

About three weeks after the first model of Cipher Device M-138 was received from the Brooklyn Depot, War Plans and Training Division placed an order for the construction of a second experimental model developed within the Division. This order[5] with the American Instrument Company, 774 Girard Street N. W., Washington, D. C., on 28 November 1933, resulted in a cost of $65.00 for the construction of one device, eventually known as Cipher Device M-138-T2. The American Instrument Company built it in accordance with verbal instructions from Mr. William F. Friedman of War Plans and Training Division. Of the three M-138 models[6] considered by the Signal Corps Board, Cipher Device M-138-T2 was the one recommended as most suitable. The changes suggested by the Board for improvement of the recommended Cipher Device M-138-T2 were

---

4. Ltr from Signal Section, New York General Depot, Brooklyn, N.Y., to The Chief Signal Officer, 4 Nov 33. AS-80A File: Cipher Device M-138.

5. Purchase Order No. SC 103407, Procurement Authority SC 4318-P-13-1381-A-541-4, 28 Nov 33.

6. Consideration by the Signal Corps Board of the three Cipher Device M-138 models is fully explained on pp.38-40.

actually made on the only model. Cipher Device M-138-T2 literally became Cipher Device M-138-T4; therefore, no photographs of Cipher Device M-138-T2 are available without the changes which make it Cipher Device M-138-T4. A brief description of the T4 model is given on p.40; a detailed listing of changes made in Cipher Device M-138-T2, is shown on p.41; and a detailed description of Cipher Device M-138-T4 is a part of Tab 19.

D. Cipher Device M-138-T3

The third experimental model of Cipher Device M-138, eventually referred to as Cipher Device M-138-T3, consists of a rectangular metal plate completely covered in red leather. The channels are composed of red leather pockets stitched on the left half of the operating surface; the right half of the operating surface contains gold guide lines and numbers (Tab 18).

Cipher Device M-138-T3 was a Navy development, adopted as standard by the Navy in early 1934 or late 1933. Mr. Friedman was of the opinion that the Navy-developed strip cipher device should be compared with the Army development before attempting a decision as to the exact form to be standardized by the War Department. Therefore, at his suggestion, the Navy Department was requested to approve the sale

of two samples of their device.[7] The Navy approved this sale to be made directly to the War Department by the Government Printing Office, which agency, in February 1934, was manufacturing these strip devices for the Navy Department.[8] The requisition for the two sample devices specified that the Navy lettering on the outside of the flap be omitted and War Department lettering substituted.

E. Cipher Device M-138-T1, M-138-T2, M-138-T3 Tested by the Signal Corps Board

In March and April 1934 Cipher Device M-138-T1, M-138-T2, and M-138-T3 were simultaneously tested by the Signal Corps Board; this test became Signal Corps Board Case No. 193 (Tab 20). As stated to the Signal Corps Board in the letter[9] presenting the case, the intended use of the device was as

---

7. W.D. requisition No. 41746: Request for 2 copies of red leather Navy strip device. The requisition is mentioned in a ltr to the Public Printer, from Lt. (jg) F.S.L. Goodwin, U. S. Navy, 15 Feb 34. AS-80A File: Cipher Device M-138.

8. These strip devices were manufactured for the Navy Dept. by the Government Printing Office on G.P.O. Jacket No. 16255. Ltr to the Public Printer from Lt. (jg), F.S.L. Goodwin, U.S. Navy, 15 Feb 34. AS-80A File: Cipher Device M-138.

9. Report on Signal Corps Board Case No. 193, 20 Apr 34. Ltr from Maj. G.L. Van Deusen, Executive OCSigO, to President, Signal Corps Board, Ft. Monmouth, N.J., 7 Mar 34. Tab 20.

follows:

> It is proposed to adopt this as a cryptographic device in tactical units down to and including division message centers, as an auxiliary means of secret communication between holders of Army Field Code.

This letter also stated that the following points were specifically presented for study and determination by the Board:

a. Speed of operation of Models 1, 2 and 3 as compared with Cipher Device, type M-94 in:

   (1) Setting up the device to a new key
   (2) Cryptographing and decryptographing.

b. Speed of operation of Model 2 as compared with Model 3 in:

   (1) Setting up the strips to a new key
   (2) Cryptographing and decryptographing

c. Relative susceptibility to errors in the case of Models 1 and 2 compared with Model 3.

d. Relative ruggedness and durability of Models 1, 2 and 3 under field conditions.

e. Relative ease in storage and transportation and resistance to damage in handling of Models 1, 2, and 3.

In making the test the Signal Corps Board collaborated with Major William F. Friedman, Signal Reserve, War Department Cryptanalyst, and with 1st Lieutenant Mark Rhoads, Signal Corps. The studies outlined in the directive letter (see a through e above) were conducted by a group consisting of one noncommissioned officer and four men, who were assigned

for this duty, under the supervision of 1st Lieutenant Mark Rhoads (Tab 20). This test resulted in the following recommendations by the Signal Corps Board:

> The board recommends that:
>
> 1. The Signal Corps Laboratories, Fort Monmouth, New Jersey, be directed to develop, as part of Project No. 86, a model similar to that of model 2 and incorporating the ideas in accordance with those contained in the CONCLUSIONS of this report.[10]
>
> 2. Models 1, 2 and 3 together with all descriptive matter and alphabets, be turned over to the Signal Corps Laboratories for use in making up the model referred to above.

F. Cipher Device M-138-T4

The fourth model of Cipher Device M-138, eventually referred to as Cipher Device M-138-T4, is an alteration and improvement of Cipher Device M-138-T2. It consists of a thin aluminum board on which are mounted 25 aluminum channels (Tab 19). The channels, which are mounted on the board rather than milled into the surface, had thin edges that "could possibly be bent by dropping a heavy object on them." This objection was overruled by the belief that "even so they could be pried up with a knife or screw driver." (Tab 20).

As recommended by the Signal Corps Board, Signal Corps Laboratories fashioned Cipher Device M-138-T4 by adding

---

10. For CONCLUSIONS to Signal Corps Board Case #193, see Tab 20.

the following changes to Cipher Device M-138-T2:

a. A felt backing.

b. A filler strip of material having the same thickness as the material used in the guides for the alphabet.

c. A straight edge slide, and

d. A strip of aluminum carrying numbers to facilitate the setting of the slide.

e. Sanding of the upper metal surfaces.

f. A protective carrying case with zipper fastener on the side.

The Signal Corps Laboratories completed the T4 model about 1 June 1934 and turned it over to the same group that made the tests in connection with Signal Corps Board Case No. 195. Lieutenant Mark Rhoads, officer in charge of the test group, reported to the Signal Corps Board favorable results of the test of the T4 model.[11] Consequently on 7 June 1934 the Signal Corps Board, reporting this matter as Signal Board Case No. 199, (Tab 21), issued the following conclusions and recommendations:

CONCLUSIONS:

The Board concludes:

a. That the operation of the device has been considerably improved by the changes that have been introduced in the model T4.

---

11. Details of the report made by Lt. Mark Rhoads, are given in Signal Corps Board Case No. 199 (Tab 21).

b. That the present model, including its carrying case, is more rugged and durable than any of the models tested in connection with Case No. 193.

c. That the alphabet strips be slightly tapered on the left end to facilitate resetting.

RECOMMENDATIONS:

The Board recommends:

a. That a cipher device similar to the model type M-138-T4 be adopted as standard for the uses specified in the above directive.

b. That in future production of this equipment the carrying case be olive drab in color and have the zipper fasteners on the end rather than on the side.

c. That the alphabet strips be slightly tapered on the left end to facilitate resetting.

On 9 July 1934, at Meeting No. 116,[12] the Signal Corps Technical Committee recommended that Cipher Device M-138 be adopted as to type and classified as standard. This action was taken as a result of Signal Corps Board Case No. 199. The SCTC minutes state that the device was intended "for use only by Signal Corps troops in division headquarters and higher units." On 21 August 1934 this recommendation was placed in effect.[13] By order of the Secretary of War, Cipher Device

---

12. Minutes of SCTC Meeting No. 116; filed, Engineering and Technical Services, OCSigO, The Pentagon.

13. Ltr to TAG (thru Ass't Sec'y of War) signd: For the CSC by Lt. Col. Dawson Olmstead, Executive Officer, 6 Aug 34. Sub: Adoption of Cipher Device, type M-138. AS-SCA File;

M-138 was classified as an adopted type, standard item of equipment. It was declared a non-essential item and the Signal Corps was charged with procurement and issue. The basis of issue was for use "only by Signal Corps troops in division headquarters and higher echelons."

Cipher Device M-138.

1. It is recommended that the above-mentioned item of equipment which is intended for use only by Signal Corps troops in division headquarters and higher echelons, be adopted as to type and classified as standard.
2. In compliance with paragraph 12, AR 850-25, the following information is furnished:
   (1) Cipher Device, type M-138.
   (2) This item replaces Cipher Device, type M-94, in division and higher headquarters and is a more secure cipher device than the M-94.
   (3) Recommend the Signal Corps be charged with the procurement and issue of this item.
   (4) Recommend this item be classified as non-essential.
   (5) Request indication of procurement clearance hereon.
   (6) This action was recommended by the SCTC in its meeting No. 116 on 9 Jul 34.
   (7) This item possesses all the required military characteristics.
   (8) No other item of equipment requires standardization or modification to effect the issue of this item.
   (9) This item is for immediate procurement and issue.
   (10) The procurement problem will not be affected.
   (11) Estimated cost per item is $25.00.

1st Ind. To: A.G. By direction of the Ass't Sec'y of War sgnd Lt. Col. John Mather, Ord. Dept., 7 Aug 34. 2nd Ind, To: The Chief Signal Officer, by order of the Sec'y of War, sgnd Robert L. Collins, A.G., 21 Aug 34. The second indorsement contains the infcrmation to which the text refers.

G. Navy-developed Model of Cipher Device M-138

When the above action was completed, the T4 model of Cipher Device M-138 was the one intended for production. In the meantime, however, the Navy Department, using the T4 model as a basis, developed a slightly different model which was considered more practical. Therefore, Specifications No. 71-716 (28 Sept. 1934) and No. 71-716A (24 Nov. 1934) (Tab 28), both of which referred to the T4 model, were cancelled in December 1934 in order to procure, instead, the Navy-developed strip board.

Briefly, the adopted Cipher Device M-138 consists of an aluminum board on which are mounted horizontally, 26 slender cylindrical rods (Tabs 22, 23). The spaces between the rods form 25 channels in which paper alphabet strips may be slid. Every fifth cylindrical rod is dark; effectively dividing the board into groups of five channels each. When the device is laid flat, it rests on four small rubber legs. It will also stand at about a 45° angle by means of a metal rod support.

H. Procurement of Cipher Device M-138

On 7 January 1935 a purchase order[14] was placed with the Bureau of Engineers, Navy, for 30 of the Navy-developed

---

14. Purchase Order No. SC-103555, R. No. 2056, Authority: SC-5367-P-1-3059-A-545-56, 7 Jan 35. AS-30A File: Cipher Device M-138.

strip boards. Under authority of this purchase order the strip boards were manufactured for the Chief Signal Officer at a cost of $15 per device for a total of $450. The Adjutant General's approval for publication of 200 copies of instructions for use of Cipher Device M-138 was given 22 March 1935.[15] The 30 devices of the initial order were received 1 April 1935[16] and on 1 July 1935 systems using them replaced Military Intelligence Code No. 10 in its capacity as a staff code,[17] that is, the new cipher system replaced the old code as a means of intercommunication between (1) the War Department and the Commanding General of a Corps Area or Department and (2) the Commanding Generals of Corps Areas and Departments.[18]

---

15. Ltr To: A.G. from Lt. Col. Dawson Olmstead, Executive Officer, OCSigO, 14 Mar 35. Sub: Printing of Instructions for Cipher Device M-138. 1st Ind., from AGO, WD, To: The Chief Signal Officer, 22 Mar 35. AS-80A File: Cipher Device M-138.

16. Memo from Maj. S. B. Akin, to Supply Division, 22 Apr 35. AS-80A File: Cipher Device M-138.

17. Ltr from Lt. Col. Dawson Olmstead, Acting CSigO, To: Commanding Generals of all Corps Areas and Departments, 25 Apr 35. Sub: Cipher Device Type M-138. AS-80A File: Cipher Device M-138.

18. On 11 Jul 34, the Sec'y of War had approved the recommendation of the CSigO to issue Cipher Device M-138 with secret alphabets and keys to the Commanding Generals of Corps Areas and Departments for current peace-time use in enciphering secret message.

Within the next few months 120 additional Cipher Device M-138's were ordered, bring the total number to 150. The price for the 120 additional devices was the same as for the original 30; namely $15.00 each, or an additional total of $1,800.00.

These 120 devices were ordered in two groups; the first group[19] of 60 on 20 August 1935 and the second[20] on 26 November 1935. The first group of 60 were ordered for distribution[21] to Army units for Class B communication with the Navy. Class B communication designated a network of reserve systems held in case of a national emergency and not to be used until placed in effect concurrently by the War and Navy Departments. After the order for 60 Cipher Device M-138's was placed to take care of Class B communications, it was decided that 60 were not enough to replace the Army-Navy Cipher No. 1 then serving for Class B communications. Therefore, more were needed and part of the second order for 60 devices was to be

---

19. Purchase Order No. SC-103607, R. No. 3717, Authority: SC-6363-P-1-3059-A-545-56, 20 Aug 35.

20. Purchase Order No. SC-103622, R. No. 3717, Authority: SC-6368-P-1-3059-A-545-56, 26 Nov 35.

21. R&W from WP&T, sgnd Friedman, to SIS, 20 Nov 35. All info. about intended distribution of the 120 devices is from this memo. AS-80A File: Cipher Device M-136.

used for this purpose. In addition, some were wanted as reserve in case of mobilization, some for training purposes, and some for actual service as needed.

Delivery of the 120 cipher devices was made by the Navy Yard to New York General Depot in May 1936,[22] and distribution was effected between June and October.

Successful operation of Cipher Device M-138 was short, for difficulties were experienced in its operation. An account of the difficulties is given in Chapter VI.

I. Rotary Alphabet Strip Cutter

Production of Cipher Device M-138 created the need for a facile method of production of the alphabet strips since they were to be changed from time to time. During the period in which the first 150 devices were being produced, the strips were cut from semi-cardboard sheets at the Government Printing Office. The cutting procedure required one hundred separate cuts per sheets, resulting in a very expensive process. Therefore, the immediate need for developing a faster and cheaper method of cutting was apparent. In June 1936 an idea had already been conceived for a rotary cutter of circular knives capable of cutting 25 of the semi-cardboard strips in one

22. Memo from Maj. Henry L.P. King, To: Supply Division, 10 Jun 36. AS-80A File: Cipher Device M-138.

revolution of the knives. The idea was conceived by William F. Friedman and under his direction a model was constructed for the Office of the Chief Signal Officer at the machine shop of the Government Printing Office. On 15 June 1936 Signal Corps Laboratories were directed by the Office of the Chief Signal Officer to prepare specification for manufacture of the cutter in accordance with instructions given by Mr. Friedman. These specifications (Tab 24) were wanted in order to have drawings of the device available in case additional cutters were necessary.

CHAPTER VI. CIPHER DEVICE M-138-A

A. Proposal for Modification of Cipher Device M-138

Almost immediate difficulty was experienced in using Cipher Device M-138, and in November 1936 plans were made for its modification. Although work was started on its successor, Cipher Device M-138-A, Cipher Device M-138 was not immediately abandoned.

The difficulty experienced by operators with Cipher Device M-138 was a binding action in the channels of the device which made it hard to slide the alphabet strips. These channels were formed by mounting 26 cylindrical rods upon the metal base whereas the 30 channels of Cipher Device M-138-A were milled into the base. The sides of the M-138-A channels were undercut, both to retain the paper strips and to permit free movement. A similar modification was made in the Coast Guard and Treasury Department devices manufactured by Price Brothers of Frederick, Maryland.

B. Original Procurement and Revision of Specifications

Definite steps to obtain cost estimates on procurement of the modified device were begun on 24 November 1936 when the Office of the Chief Signal Officer requested the Signal Corps Laboratories to estimate the cost of the new device,

when purchased in lots of 200, as compared with the cost of the old device. Instead of making their own estimate, Signal Corps Laboratories sent requests for cost estimates to several manufacturers[1] who took several months to reply. Tophams, Incorporated which offered the lowest bid at the rate of $11.00 per device, did not send its reply until 6 February 1937. The estimates verified the practicality of procuring the new device; therefore, the Signal Corps Laboratories proceeded with revision of the specifications. Specification No. 71-716, dated 3 January 1935, which covered Cipher Device M-138, became Specification No. 71-716-B, dated 7 April 1938, for Cipher Device M-138-A[2] (Tab 28). As work progressed during 1937 on revision of the Specification to incorporate the new-type channel, additional modifications were recommended to Signal Corps Laboratories by Signal Intelligence Section of Research and Development Division, Office of the Chief Signal Officer. The additional recommendations were as follows:

---

1. The two manufacturers which submitted bids were the Dicke Toole Co. of Downers Grove, Ill., and Tophams, Inc., 3rd and Eye Sts, N.E., Washington D. C. Tophams, Inc. gave the lowest cost estimate. Using the extrusion process, Tophams, Inc. quoted an approximate cost of $11.00 each in lots of 200.

2. Specifications covering CD M-138-A: Specification No. 71-716-B, 7 Apr 38; Specification No. 71-716-B, 17 Apr 38, Amendment No. 1; Annex Issue No. 7 to Specification No. 71-716, 25 Oct 40.

. . . It is desired that the following modifications be made in the design of the M-138:

a. The stop bars at the right and left of the device to be increased in width to approximately 1/4 inch so that the space between the stop bars shall be equivalent to the space occupied by 53 letters, as in the sample alphabet inclosed.

b. Consider for the purpose of what follows that the visible part of the device will be 53 columns wide and that these columns will be counted from left to right. Above the 1st and 53rd columns should appear the caption "CLEAR TEXT"; above the 27th column should appear in red the caption "DO NOT COPY." Each even[2a] numbered column, except 1, 27, and 53, should have at top and bottom a black vertical line. These marks are for the purpose of assisting the cryptographer in aligning the guide rule.

c. The T-square arrangement now proposed by your Laboratories for the guide rule is more complicated than necessary. It is desired that a slider running in a groove at the top and a similar groove at the bottom be substituted instead of the arrangement proposed by your Laboratories. This slider to be $\frac{1}{2}$ inch wide on the face of the device and 1-$\frac{1}{4}$ inches wide at the slots. Thus when the slider is in its extreme left (or right) position the space between the stop bar and the near edge of the slider shall be 3/8 inch. When "CLEAR TEXT" is set up in this space the same "CLEAR TEXT" shall also appear in the 27th column headed "DO NOT COPY."

Detailed drawings to be used as part of the Specifications were made and revised by Signal Corps Laboratories during 1937 and the nomenclature, Cipher Device, type M-138-A[3], was assign-

---

2a. Apparently an error. Document not available for checking.

3. Classification of Cipher Device M-138-A as standard was considered the same action as classification of Cipher Device M-138 as standard. (pp. 41-43).

ed by the Nomenclature Section, Office of the Chief Signal Officer, at the request of Research and Development Division, Office of the Chief Signal Officer on 8 June 1937. However, procurement was not seriously considered because funds had not been specifically allotted for the purpose.[4] 1938 was evidently the year for service testing and original procurement of the new device. All details on how the original devices were procured and on service testing are missing; but it is known that 224 were distributed to holders on 9 September 1939 (Tab 36).

C. Procurement of Additional Cipher Device M-138-A

Production of Cipher Device M-138-A in some quantity began in the fall of 1940[5] when 550 devices were ordered from the Widin Metal Goods Company,[6] Garwood, New Jersey, for $8,250.[7] (Order No. 1070-Ny-41, dated 27 September 1940.)[8] The request

4. R&W, from R&D Div., to WP&T Div., 9 Feb 37, 10 Feb 37. AS-80A File: Cipher Device M-138-A.

5. Memo SIS for Supply, 3 Jul 40. This memo is the purchase request for 550 devices. Same file as footnote 4.

6. Memo SIS for Supply, 6 Jan 41. This memo states that 550 M-138-A's had been ordered from the Widin Metal Goods Co. File: same as above.

7. Memo Col. S. B. Akin for Executive Office, OCSigO, 24 Jun 40. Request for approval of funds which included the $8,250 for 550 M-138-A. A note in pencil sgnd by Col. A. B. Akin states that Gen. J. O. Mauborgne approved the request on 1 Jul 40. File: same as above.

8. R&W from SIS to Supply, 9 Jul 41; File: same as above.

for approval of funds for the 550 devices stated that the funds would be used to provide Cipher Device M-138-A "for issue to posts and stations not already having them, posts and stations established during the present emergency, and the National Guard Divisions."[9] Later, the order was increased by 60 bringing the total requested to 610. On 6 January 1941 Signal Intelligence Service requested Supply Division to increase the order again, this time by 120 devices for the following reasons:[10]

(a) The increase in the contemplated size of the Army over the previous estimates.

(b) The time required for the procurement of these devices (approximately 6 months).

(c) A threatened shortage of aluminum from which these devices are made.

The Signal Intelligence Service remarked in every memorandum that the devices were urgently needed. The urgency was undoubtedly caused by plans for expansion of the Army as evidenced by the first Selective Service, prefacing World War II, in October 1940. Delivery on these orders was begun about June 1941.

---

9. All details on bidding and on why the Widin Metal Goods Co. was selected as the manufacturer are missing.

10. Memo SIS for Supply, 6 Jan 41. AS-80A File: Cipher Device M-138-A

~~SECRET~~

By request, the manufacturer delivered the new Cipher Device M-138-A's as they were completed. For this reason, it was only gradually discovered that almost all of the 550 devices of the original order were delivered in a defective condition and had to be returned to the manufacturer for repair.[11] At first, it was hoped that the devices could be made usable by local repair without return to the Widin Company but this proved impossible. The defect was caused by use of a damaged die which produced an improperly milled third channel.[12] The die was damaged in production. The correspondence does not actually state the following but implies that although Widin Metal Goods Company produced the Cipher Device M-138-A, the Aluminum Company of America furnished the damaged die[12] as well as the aluminum. Other minor defects in the form of burrs[13]

---

11. Ltr Capt. Charles D. Cushman, Contracting Officer to Widin Metal Goods Co., Garwood, N.J., 15 Sep 41. Compare with ltr to The Chief Signal Officer from Maj. Robert Walsh, 4 Oct 41. File: same as footnote 10.

12. Memo Wesley Hermanson, Jr., R. Eng., no date, Letterhead N.Y.S.C. Procurement District, Brooklyn, N.Y. for Mr. Kyne. "The part of Cipher Device M-138-A, which was defective, is made by the extrusion process. The die used to make the lot covering the 550 cipher devices on Order 1070-Ny-41 was damaged during production. The attention of the Aluminum Co. of America, in whose possession the die remains, has been called to this defect. The Aluminum Co. will repair the die and the increase of 60 cipher devices on Order 1070-Ny-41 will be free from this defect...." File: same as above.

13. SIS, R&W Action 3 to S&L, 7 Sep 41. File: same as above.

~~SECRET~~

in the various channels were also discovered. Even small burrs hindered the movement of the alphabet strips but they could be readily removed by using an ordinary pocket knife.[13]

In the fall of 1941 an additional order[14] for 518 Cipher Device M-138-A's was placed. This order was marked due 4 April 1942 but has not been confirmed as completed.

PROCUREMENT OF CIPHER DEVICE M-138-A

Shipment completed:

	On hand, 9 Sep 39	224
	Rec'd on Order 1070-Ny-41 DP 41-155 (27 Sep 40)	550
1-27-42	Increase in Order 1070-Ny-41 DP 41-804	60
3-3-42	Rec'd on Order 3338-Ny-41 DP 41-1139 (Date on purchase request for this order: 1 Jan 41	120
		954

Due: 4-4-42 (not confirmed as completed)	Order 6011-Ny-41 DPs 41-3288 and 41-3202	518
	Total procured	1,472

D. Cancelled Order for 4,873 Cipher Device M-138-A

Mass production of Cipher Device M-138-A was about to begin in early 1942 with an order of 4,873[15] at $16.00 each

---

14. Order No. 6011-Ny-41, DPs 41-3288 and 41-3202 (Not confirmed as completed).

15. Order for 4,873 Cipher Device M-138-A's, DP 42-M-817, Funds Resume SSA-P-5-30, FY 42-43, $77,968.00, 30 Mar 42, (CANCELLED). AG-80A File: Cipher Device M-138-A.

for $77,968.00 (30 March 1942) when difficulty in the form of shortage of aluminum was encountered. The order for the devices was stopped in the Philadelphia Signal Corps Procurement District. The procurement office received only two bids, one of which was from the Widin Metal Goods Company. Their bid was accompanied by a letter which stated that the War Production Board had disallowed their request for allocation of aluminum. In view of the fact that production of 4,873 devices would have required approximately 11 tons of aluminum, manufacture of the devices from this metal was impossible.[16] Therefore, the Signal Intelligence Service took action to cancel DP 42-M-817, which was the order for the 4,873 aluminum Cipher Device M-138-A.[17] The replacement of Cipher Device M-138-A's by substitute devices is discussed in CHAPTER VII, "Overcoming the Aluminum Shortage."

E. Patent

The basic U. S. Patent (No. 2,395,863) covering strip cipher devices with variable alphabets sliding within grooves or channels was granted to Mr. William F. Friedman. The application[18] for the patent was filed on 13 October 1939. The first

---

16. Capt. S. H. Franklin, R&W Action 1 to SIS (Major Cook). Proc. SPSRP-9-M, 14 Apr 42. AS-80A File: Cipher Device M-138-A.

17. Ibid. Action 3.

18. Information concerning action of Patent No. 2,395,863 was furnished in writing by Henry B. Stauffer, Chief, Patents Section, AS-70, 20 Jan 47. File: Same as above.

Patent Office action, 9 November 1939, rejected all claims. The rejection, notwithstanding a large number of United States and foreign patents cited by the Patent Office Examiner, was "weak, and, in view of a response, 7 May 1940, which amended the application in relatively minor particulars, the application was allowed 18 June 1940 with 19 claims.... The patent was not, however, permitted issue in 1940 because of security considerations, but instead was retained in the Patent Office in secret status until 5 March 1946.... The invention and the application were assigned to the Government while the application was on file, but reassigned to the inventor when the patent was issued, and the Government now retains merely a nonexclusive license to manufacture and use the device without payment of royalty."[19]

19. Ibid.

CHAPTER VII. OVERCOMING THE ALUMINUM SHORTAGE

A. Cipher Device CSP 845 (Plastic)

The Navy devices, used to substitute for the unobtainable aluminum Cipher Device M-138-A, were known as CSP 845 (Plastic) (Tabs 29, 30). On 22 October 1942 a purchase request[1] for 5,000 Cipher Device CSP 845's (Plastic) was sent by Signal Security Branch to Purchasing Branch of Procurement Division. The actual purchase order[2] for the 5,000 devices, dated 9 December 1942, designated the total cost as $45,000.

Substitution of Cipher Device CSP 845 for Cipher Device M-138-A did not result, however, in the first purchase of the Navy devices by the Army. The first purchase request[3] made on 22 January 1942 (from SIS to Procurement Division) was for 1,200 devices to be procured from the Bureau of Ships, U. S. Navy, at a cost of $8.50 each. These devices were to be used for the dual purpose of joint communication with the Navy

---

1. SSB R&W Action 1 Maj. Earle F. Cook to Purch. Br., Proc. Div., OCSigO, Thru: Sched. Br., 22 Oct 42. AS-80A File: CSP 845.

2. Purchase Order for 5,000 CSP 845s; cost $45,000, Order No. 496-OCSigO-43; Procurement Authority: SC-3247-P-120-09-A-0605-23; 9 Dec 42. File: Same as above.

3. Purchase Request, to Procurement from Lt. Col. R. W. Minckler, SIS, 22 Jan 42. Purchase Order No. 132-OCSigO-42, Procurement Authority of estimated $10,200; SC 801 P 5-30-A-0605-12, 9 Feb 42. File: Same as above.

and to augment the supply of Cipher Device M-138-A.

B. Unsatisfactory Service of Plastic CSP 845

In 1942 and 1943 the placement of Army troops all over the world brought about wide distribution of the plastic Cipher Device CSP 845. However, the plastic strip boards did not prove satisfactory, particularly in tropical climates where the hot, moist weather produced warping of the board. Complaints concerning the unworkability of CSP 845 (plastic) began to appear in April and May 1943 and continued into 1944.[4] Although steps were taken at once for replacement of

---

4. Examples of complaints concerning CSP 845 (Plastic):

a. Complaint from Hq. Area Service Command, Air Task Force, Office of the Commanding Officer, Sgnd. Col. R.L. Wood, Commanding; To the CSO thru Hq., Trinidad Sector and Base Command, Port of Spain, Trinidad, B. W. I., May 1943.

1. Numerous reports from Air Base Headquarters under this command have been received to the effect that the plastic type code board CSP 845 has proven very unsatisfactory for cryptographic work.
2. Strips used in the board are very quickly worn and torn so that they are unserviceable. The celluloid strips last a little longer than the paper ones, but they too are soon damaged to the extent that encoding and decoding is difficult. Boards have been tried with and without the ball bearing. Results are the same; namely, the code strips become unusable in a very short time.
3. It is recommended that subject boards be replaced with standard type boards and that no additional boards of the new type be procured.

b. Trip Report Sgnd. Lt. Col. Earle F. Cook. Memo to Chief, "C" Branch, SSA; Subject: Observations on Cryptographic Communications--Southwest Pacific Area, South Pacific Area, Hawaiian Dept.

the unserviceable plastic devices, distribution of the replacements was necessarily gradual.

To make the necessary replacements, occasioned by the unsatisfactory service of plastic CSP 845, and at the same time overcome the problem of aluminum shortage, considerable redistribution of strip boards became necessary. The following plan was effected: All metal boards (both M-138-A and CSP 845) were recalled from holders in the continental United States (19 July 1943) and sent overseas to holders who were having the most serious trouble with plastic devices. In tropical climates, the worth of the plastic devices was

---

> . . . Considerable use is made of strip systems, particularly in the Southwest Pacific Area. The chief difficulty arises with the plastic CSP 845. At no place in the Pacific Area is the operation of this device satisfactory. Attempts have been made to improve the operation by oiling the device and waxing the strips. Humidity is such, however, that the friction between the strips and the plastic device does not permit satisfactory operation. A satisfactory substitute must be found for this plastic device . . .
>
> c. From the Communication Security Officer, 6th Service Command, Chicago, Illinois.
>
> 1. It is requested that two (2) additional cipher devices, other than plastic CSP 845, be sent to the Signal Officer, Camp Ellis, Illinois.
>
> 2. At present he has one (1) plastic CSP 845 . . . Although the ball bearings have been removed, it still causes great difficulty in the operation of the strips.

negligible. The metal boards returned by holders in the continental United States were replaced by a newly-designed wooden board with the Army title: Cipher Device M-138-A (Wood), Short title: SIGWOWO. It was always called - even in official documents - by its short title to provide easy distinction from its metal counterpart.

C. SIGWOWO

The wooden SIGWOWO, made of Honduras mahogany, had a simple development. Its inception, about January 1943, was instigated by the shortage of aluminum. The original intention was to replace both the plastic and aluminum Cipher Device CSP 845 in the continental United States and to release the replaced devices for field use. Since the plastic devices were unserviceable, the SIGWOWOs replaced only metal devices in the continental United States, and released these metal boards for replacement of plastic devices in tropical areas overseas.

Fifty devices were purchased for experimental purposes just prior to November 1942 and were tested at the Arlington Hall Message Center where they gave satisfactory service. Therefore, on 28 November 1942, approval of the purchase of 2,000 wooden devices for $14,000 was requested by Code Com-

pilation Section.[5] The devices were constructed by H. W. Heslop & Bros. (Lumber Company located at 724 Q St., S. W., Washington, D. C.) from specification drawings[6] conceived within the Signal Security Branch. When placed in service, as described above, SIGWCWO also proved unsatisfactory in the field because of friction of the paper strips on the wood and warping of the board.

D. Cipher Device CSP 845 (Metal)

Fortunately, in September 1943, aluminum again became available so that it was possible to order 8,000 metal CSP 845 devices from the Navy Department.[7] The contract was for 8,000 devices at $80,000, delivery to begin not later than 15 December 1943, at the rate of 1,000 per month.[8] Delivery on these

---

5. Memo Lt.Col. Earle F. Cook, Chief, Code Compilation Section, to Col. F. W. Bullock, OIC, SIS: 28 Nov. 42; Sub: Cipher Boards; AS-80A File: Cipher Device CSP-845.

6. Contract W-946-SC-24; Order 1573-SC-43; 23 Feb 43, H. W. Heslop & Bros.

7. Memo Lt. Col. Kenneth Kuhn for Chief, Security Division, 6 Dec 44, Sub: Disposition of CSP 845 (Plastic) SIGWCWO, M-138 and M-138-A. AS-80A File: Cipher Device CSP 845.

8. Purchase Request No. 44-682 & Amend. A, To: Philadelphia Procurement District, for 8,000 CSP 845s (Aluminum), Procurement Authority given on purchase request: P 120-09 SSA 42-44, 13 Sep 43. A notation on this purchase request gives the information that this equipment was to be procured by Interdepartmental Procurement through the Navy Dept. In accordance, procurement was affected through Interdepartmental Order No. Phila-682-A-44 from Philadelphia Procurement District to U. S. Navy - Bureau of Ships, 1 Oct 43. Procurement Authority given on Order Phila-682-A-44 is 3-3765 P 120-09 A 212/40605.

devices was completed 13 October 1944.[7]

This order made it possible not only to replace all SIGWOWOs and all plastic CSP 845's but, for the sake of uniformity, to recall Cipher Device M-138-A, which were entirely serviceable.

The Signal Security Agency declared the following devices obsolete: CSP 845 (plastic), SIGWOWO, M-138, and M-138-A. A letter implementing this action was sent to holders on 20 December 1944.[9]

E. Summary of Procurement Problems

Summarily, the aluminum shortage made a complicated problem of procurement and distribution of strip boards. Briefly, the story is that the aluminum strip board, Cipher Device M-138-A, proved most satisfactory in service but shortage of the metal forced plans to discover another satisfactory material. Two materials were tried. An attempt to use wood resulted in a strip board called SIGWOWO, which was made of Honduras mahogany. An attempt to use plastic resulted in the purchase of 5,000 strip boards, called CSP 845, from the Navy. Both boards proved unsatisfactory in service. However, ingenious redistribu-

---

9. Ltr No 532, SPSIC-2 sgnd. by Maj. Russel H. Horton, SSB and for the Chief Signal Officer by Maj. Gen. Frank E. Stoner, Chief, Army Communications Service, 20 Dec 44. AS-80A File: Cipher Device CSP 845.

tion plans bridged the gap until aluminum again could be obtained. The redistribution worked out as follows:

(1) All metal boards were recalled from holders in continental United States (19 July 1943).

(2) Metal boards of (1) above were distributed to overseas holders. (Fall of 1943 to early 1945.) (Holders in tropical areas had to be serviced with metal boards before other holders because hot, moist climates caused the most serious difficulty with plastic.)

(3) Plastic boards were recalled from overseas as rapidly as the released metal boards of (1) above made replacement possible. (From summer 1943 to early 1945.)

(4) Holders in continental United States were given wooden boards, SIGWCWO, to replace the metal boards which they released for the purpose of overseas shipment. (Shipped July 1943.)

In September 1943 aluminum again became available and allowed an order from the Navy of 8,000 aluminum Cipher Device CSP 845. The completion of delivery of the 8,000 metal devices in October 1944 permitted complete distribution of the metal strip board, CSP 845, with recall of, and declaration as obsolete, of all other strip devices. The approximate number of all devices procured between January 1935 and September 1943 is given in Tab 33. A chronological outline of the procurement of Strip Cipher Devices composes Tab 34.

F. Storage and Disposal of Obsolete Strip Boards

All the Cipher Device M-138's and M-138-A's and SIGWCWOs

were returned to the Signal Security Agency.[10] The Cipher Device M-138-A's were stored there for emergency issue. Five Cipher Device M-138's were retained by Signal Security Agency for historical purposes and the remainder salvaged for their metal content. Signal Security Agency obtained SIGWCWOs for salvage of the Honduras mahogany of which they were constructed. All damaged Cipher Device CSP 845's (Plastic) were collected and destroyed in the Theater. All undamaged Cipher Device CSP 845's (Plastic) were returned to the Navy for subsequent distribution to the British Admiralty. This action was to implement the Navy program of supplying the British Admiralty with Cipher Device CSP 845's (Plastic) for "distribution to all British services."[11]

G. Status of Registry and Security Classification and Transfer of Responsibility for Storage and Issue of Strip Cipher Devices

The status of registry and security classification of the various strip boards was so changeable that problems arose concerning accountability of the devices. Cipher Device M-138

---

10. All information in this paragraph, unless otherwise designated, is from Memo, Lt. Col. K. Kuhn for Chief, Security Division, 6 Dec 44. Sub: Disposition of CSP 845 (Plastic), SIGWCWO, M-138, and M-138-A. AS-8OA File: Cipher Device CSP 845.

11. Ltr Director of Naval Communications to CSO, Attn. Col. W. Preston Corderman, Chief, Signal Security Branch, 30 Nov 44. Sub: Strip Cipher Devices (Plastic), request for. AS-8OA File: Cipher Device CSP 845.

was issued as a CONFIDENTIAL, registered device with the short title, SIGDOV. However, Cipher Device M-138-A was issued without being either registered or classified. Consequently, on 3 March 1941, the classification of Cipher Device M-138 was cancelled. The reason for cancellation of the classification was given in the request to The Adjutant General as follows: "Authority is requested to cancel the confidential classification of the Cipher Device M-138 since the Cipher Device M-138-A, a similar device, is unclassified."[12] This change of status caused no difficulty.

Another change of classification status was required when Cipher Device CSP 845 was issued. Since this same device was issued by the Navy as CONFIDENTIAL and registered, it was, for the sake of conformity, also issued by the Army as CONFIDENTIAL and registered. The confusion occurred when, on 21 September 1943, the Director of Naval Communications effected, by memorandum, cancellation of the classification of CSP 845, thereby requiring no accountability for the Navy strip board. When Army holders became aware of the Navy memorandum, many of them assumed that it applied to all Cipher Device CSP 845's

---

12. Ltr to AG from Clyde L. Eastman, Acting CSO. Sub: Cancellation of Classification of M-138. 1st Ind. to CSO from WD, AGO, 4 Mar 41. AS-80A File: Cipher Device M-138-A.

~~SECRET~~

and ceased accounting for the Army-issued devices. The problem grew more complicated throughout 1944 because Overseas Naval Issuing Offices issued unclassified, unregistered Cipher Device CSP 845's to Army units upon request. The result was that Army units held some devices for which they must account as classified and registered, and others for which no accounting was required. The natural remedy was, of course, again to provide conformity with the Navy by removing classification and registry from the Army devices. This was done (Nov 1944), but in order not to create a new problem by applying this remedy, a special exemption from routine property accountability of the newly unclassified items had to be obtained at the same time. Removal of classification and registry made the strip devices equal to ordinary items of property, thereby removing responsibility for storage and issue from the Signal Security Agency. Since the Signal Security Agency handled associated cryptographic materiel such as alphabet strips and key lists, it was highly undesirable that responsibility for storage and issue of the devices themselves be removed from the Agency. Therefore, the following authority was requested by Signal Security Agency on 16 November 1944 (Tab 35) and approved by command of Lt. General Somervell, Commanding General, Army Service Forces:

~~SECRET~~

1. It is requested that authority be obtained from the Commanding General, Army Service Forces to exempt the CSP 845 and all other strip cipher devices from property accountability upon removal of the present classification and registry, and that the Signal Security Agency be charged with storage and issue of the devices if this authority be obtained.

Channels of authority and other details concerning "Removal of Classification and Registry and Exemption from Property Accountability," are given in photostats of the actual correspondence (Tab 35).

CHAPTER VIII. DISTRIBUTION OF STRIP SYSTEMS

A. General

By the fall of 1939, when approximately 375 strip cipher devices had been procured, Cipher Device M-138 and M-138-A were distributed through all levels of command from the War Department down to and including posts, forts, depots, and arsenals (Tab 36). However, peacetime requirement kept holders of War Department systems at less than 300. By the fall of 1940, plans for expansion of the Army increased requirements (pp. 52-55) and 550 devices were ordered; however, delivery of these devices was not begun until June 1941, only five months before the attack on Pearl Harbor. Early 1942 found the Signal Corps frantically attempting to get aluminum for procurement of almost 5,000 strip devices (p. 56).

Although strip devices had the disadvantage of being slow to operate, they offered several advantages over high-grade machine systems, in that they were less expensive to procure, easier to distribute because of their small size, and provided less material for compromise in case of capture. Therefore, practically every Army establishment authorized to hold cryptographic material held strip devices, unless they were mobile or front-line units recognizably unable to operate strip boards. Although this wide distribution (Tab 36) of

strip devices is not an inherent proof of how frequently they were used, it does indicate that the contribution of strip systems to cryptographic communication is most significant.

Strip systems were used primarily in two ways during World War II: (1) as stand-by systems in case the normal means of communication, which was usually a machine system, became inoperative for any reason; (2) as a normal means of communication between holders authorized and those not authorized a high-grade machine system as well as a means of communication among holders not authorized a high-grade machine system.

B. Strip Systems as Stand-By Means of Communication

By the fall of 1943 when the orderly plan of the cryptonet began to have its effect upon the unwieldy growth of classified communications, practically every normal system[1] was provided with a separate stand-by strip system according to the original cryptonet plan as outlined in Cryptographic Communications, (short title: SIGWHY). After the cryptonet plan had been in use for about a year and a half, it was discovered that many of the stand-by and emergency systems were

---

1. For explanation of the terms "normal, stand-by, and emergency" see Cryptographic Communications, 1943 (short title: SIGWHY).

so seldom used as to make their issuance a waste of production effort. Therefore, about six months before the end of World War II, the flexible cryptonet plan was adopted and a new policy for issuing stand-by systems was placed in effect. For both world-wide and theater cryptonets the new policy became that of allowing the same system, which was usually a strip system, to stand by for two or more normal systems or even to allow one normal system to stand by for another normal system. In some cryptonets, it was possible to discontinue stand-by strip systems altogether. The policy was thoroughly dependent upon proven trends in traffic load, possibility of breakdown, number of systems held, etc. Examples of the new trend of eliminating rarely used systems or making them do double duty are given in the next paragraph and in Tab 37.

In Cryptonet 33, the special Security Representatives Cryptonet, six strip stand-by systems were issued at first. Later, in early 1945, all stand-bys were discontinued and "33" became an "ABA only" net. The net was issued without stand-bys with the understanding that Security Representatives would always be located at headquarters holding other high-grade systems which could be used as stand-bys in case Net 33 became inoperative. In February 1945 the stand-by strip systems in Cryptonets 12 and 13 were discontinued since the

distribution scheme by that time precluded the necessity for individual stand-by systems in these cryptonets. In several of the cryptonets the pattern for issuing stand-bys became that of allowing a normal strip system provided for non-holders of SIGABA, or some other high-grade machine, to do double duty by acting, at the same time, as a stand-by system for a normal SIGABA or high-grade machine system.[2] Examples of this trend can be found in Cryptonets 21, 22, 23, and 27 (Tab 38).

C. Strip Systems as Normal Means of Communication

Strip systems, both during World War II, and also at the present time, are a very important means of communication,

---

2. Ltr No 549, SPSIC-2, To: All Holders of Cryptonet 12 and 13. Sgnd For the CSO by Maj. Gen. Frank E. Stoner, Chief, Army Communications Service and Lt. Col. K. Kuhn, SSB, 12 Feb 45. Sub: Discontinuance of Destruction of Stand-by Alphabet Strip Systems in Cryptonet 12 and 13.
   1. In accordance with the Chief Signal Officer's program of eliminating cryptographic systems which are rarely used and for which a necessity no longer exists, the stand-by alphabet strip systems in cryptonets 12 and 13 are being discontinued. The distribution scheme of these two cryptonets now precludes the necessity for individual stand-by systems.
   2. Under the cryptonet plan, all holders of Cryptonet 12 hold Cryptonet 13, and all holders of Cryptonet 13 also hold Cryptonets 14 and 15. If for any reason, a normal system in Cryptonet 12 becomes inoperative, the normal system in Cryptonet 13 can be used. Similarly, if the normal system in Cryptonet 13 is inoperative, the normal systems in Cryptonets 14 and 15 can be used.

especially for holders not authorized to use SIGABA or some other high-grade cipher machine. For example, the general world-wide cryptonet had a strip system as the normal means of communication. This strip system, No. 1501, was held by almost all Army organizations authorized to hold strip systems (Tab 37). The widely distributed System 1501 permits almost any Army organization to communicate with any other but its security is protected by the fact that it is used only for unusual situations. That is, if a need for habitual communication between places holding in common only System 1501 is anticipated or discovered, a Cryptonet is organized or a system issued to take care of such traffic.

Another widely-held normal strip system was System No. 999, which was not technically in a Cryptonet. It became effective on 1 August 1945 to furnish a world-wide replacement for the War Department Telegraph Code, 1942, (SIGARM). It was designed for the RESTRICTED traffic of Army establishments which used Cryptcnets 15 and 17 for CONFIDENTIAL and SECRET messages. System No. 999 was discontinued on 1 January 1947.

During World War II, in the Military Attache Net, strip systems were used by the attaches both for normal communication with each other and for communication with the War Department radio station (WAR) at Fort Myer, Virginia. The

exception to this was The Military Attache, London, who held SIGABA and used it for communication with WAR. On 1 May 1945 one-time systems (usually one-time pads) were provided each Military Attache as isolation systems for communication with WAR. Although strip systems were approximately as widely held after the introduction of one-time isolation systems, they were much less frequsntly used since Military Attaches have a great deal more communication with the War Department than with each other.

Generalization about strip systems is difficult since it is necessary at times to mention specific systems. A few have been mentioned in the text above. To go into greater detail concerning the remainder would make the present volume too large. The alternatives are to avoid mention of specific systems or to write an additional volume. Therefore, a compromise has been attempted in Tab 38 by expanding the subject, although not to its limits. While the material in Tab 38 is an outline of the cryptonet strip systems, it is intended not as a detailed study of each system but as a means of adding to the general concept of the subject. In addition to the cryptonet strip systems outlined, there were a large number of strip systems issued independent of the cryptonets.

Figure 4

BEGINNING OF TWO LINES ENCIPHERED ON THE SAME GENERATRIX

	1	2	3	.	.	.	25
			P	.	.	.	
			Z	.	.	.	R
			C	.	.	.	C
		S	J	.	.	.	P
		Z	Y	.	.	.	Q
Plain:		L	(E)	T	.	.	. T ←
		F	B	R	.	.	. V
		H	I	M	.	.	. L
		U	K	B	.	.	. O
		J	G	V	.	.	. J
		M	M	G	.	.	. S
		N	J	F	.	.	. M
		X	T	H	.	.	. B
		P	D	N	.	.	. W
		W	O	E	.	.	. F
Cipher:		O	(Y)	I	.	.	. G ←
		I	L	S	.	.	. N
		D	Q	K	.	.	. X
		S	R	L	.	.	. I
		Y	F	N	.	.	. U
		Q	X	X	.	.	. H
		E	W	O	.	.	. E
		B	N	U	.	.	. Z
		A	V	Q	.	.	. D
		T	H	D	.	.	. K
		G	P	A	.	.	. A
		V	U		.	.	. X
		K	C		.	.	.
		C	A		.	.	.
		R			.	.	.
		Z			.	.	.

STRENGTH

	1	2	3	.	.	.	25	
			H	.	.	.		
			W	.	.	.		
			E	.	.	.		
			I	.	.	.		
	O		S	.	.	.	H	
	I	J	K	.	.	.	E	
	D	Z	L	.	.	.	Z	
→	T	(N)		.	.	.	P	Plain
	Y	B	X	.	.	.	K	
	U	I	O	.	.	.	A	
	Q	K	U	.	.	.	X	
	E	G	Q	.	.	.	R	
	B	M	D	.	.	.	C	
	A	J	A	.	.	.	D	
	S	T	P	.	.	.	Q	
	G	D	Z	.	.	.	T	
	V	O	C	.	.	.	V	
→	X	(Y)	J	.	.	.	L	Cipher
	C		Y	.	.	.	O	
	R		T	.	.	.	J	
	Z		R	.	.	.	S	
	L		M	.	.	.	M	
	F		B	.	.	.	B	
	H		V	.	.	.	W	
	U		G	.	.	.	F	
	J		F	.	.	.	G	
	M			.	.	.	N	
	N			.	.	.	X	
	X			.	.	.	I	
	P			.	.	.	U	
	W							

WEAKNESS

Two variable factors:

1. 25 mixed alphabets (1 2 3...25)
2. Choice of 25 different letters as cipher-text letter for each plain-text letter. (In first alphabet, L could have been enciphered by F, or by H, or by U, or by J, or by M...etc, instead of by O as in the example.)

Constant factor:
In left-hand example: 10 letters between L and O in the 1st alphabet, 10 letters between E and Y in the 2d alphabet, 10 letters between T and I in the 3rd alphabet ... 10 letters between T and G in the 25th alphabet. In right-hand example: the line shown was enciphered on the same generatrix, producing a constancy of the interval 10. There are 10 letters between T and K, in the 1st alphabet, 10 letters between E and Y in the 2d alphabet, 10 letters between N and J in the 3rd alphabet...10 letters between P and L in the 25th alphabet.

CHAPTER IX. SECURITY OF STRIP CIPHER SYSTEMS

A. General

The cryptographic strength of the disk or strip cipher is based upon the variable factors which it provides, namely:

(1) Encipherment by at least 25 different mixed alphabets (see example on opposite page; Fig. 4).

(2) A choice of 25 different letters for each plain-text letter (see example on opposite page; Fig. 4).

The cryptographic weakness of the strip or disk cipher is the constancy of the interval[1] between the letters of any one plain-text alignment and the letters of its cipher-text generatrix.[2] The danger of unauthorized reading arises when more than one plain-text line of letters is enciphered on the same generatrix.[3] (See example on opposite page; Fig. 4).

---

1. Interval - In this case, number of letters in each alphabet between the plain-text letter and its cipher-text equivalent. See example on opposite page; Fig. 4.

2. Generatrix - Because of the interdependence of a plain-text line of letters and its cipher text, such lines of plain and cipher text have come to be known as generatrices, in other words, one results from the other or is generated by the other.

3. That is, when, in the alphabets used to encipher, more than one plain-text line of letters is enciphered by letters which are the same number of letters from the plain-text letters. See example on opposite page; Fig. 4.

If enough lines enciphered on the same generatrix are determined, not only can the message be read, but the alphabets used to encipher can be reconstructed. Therefore, all security improvements of the disk and strip cipher were designed either to prevent or disguise the appearance of this constant factor. Opinions concerning what was necessary to prevent or disguise this factor changed through the years. In general, the security requirements became more rigid.

Security improvements made in the use of disk and strip cipher systems are chiefly concerned with the following elements:

a. Rearrangement, replacement, and supersession of alphabet strips.

b. Selection of generatrix.

c. Message length limitation.

d. Channel elimination.

e. Split generatrix.

f. Change from fixed to variable number of channels eliminated.

g. Change from channel elimination to strip elimination.

Each of these elements is discussed in detail in the paragraphs which immediately follow, beginning with the earliest years of use (by the Army) of the strip cipher principles of encipherment. In addition, the security changes appearing

in the successive editions of the comparatively recent instructional series are outlined in chart form in Tab 39. The documents of this series bear the short titles, SIGUHR, SIGUHR-2, SIGUHR-3, and SIGUHR-4. The earliest was SIGUHR, effective April 1942; the second was SIGUHR-2, effective April 1943; the third was SIGUHR-3, effective March 1945; and the fourth was SIGUHR-4, effective July 1945. For list of earlier editions of operations instructions, see Tab 41.

B. Rearrangement, Replacement, and Supersession of Alphabet Strips

One security requirement, which was introduced at the beginning and maintained through the years, was periodic rearrangement of the alphabet disks or strips. The frequency with which they were reassembled did not remain the same. During the period when Cipher Device M-94 was effective, the alphabet disks were rearranged only infrequently.[4] At least

4. Infrequent change of the alphabet disks does not indicate as great a lack of insight into the security limitations of Cipher Device M-94 as a brief backward glance might purport. First, the device was intended only for field use and secondly, early instructional material (1929) contains the following information on security limitations and rearrangement of alphabets:
"52. NECESSITY FOR KEY AND PROVIDING FOR CHANGES THEREIN. - a. Messages cryptographed by the same sequence of alphabet disks can remain secure against solution by a well-organized and efficient enemy cryptanalytic section for only a relatively short time. It is impossible to state exactly how long, because solution depends upon a number of variable factors; a conservative estimate would place the minimum at 6 hours, the maximum at 2 or 3

by 1939, after Cipher Device M-138 had been adopted, daily rearrangement of the disks became the rule.

Perhaps the most momentous of all security improvements was that which introduced changeable paper alphabet strips instead of unchangeable aluminum alphabet disks -- most momentous because it resulted in complete redesign of the form of the device. To actualize this change, Cipher Device M-94 was superseded cryptographically by Cipher Device M-138.[5]

After ability to replace the alphabet strips was added the ability to rearrange them. The frequency with which they were replaced and rearranged had an evolution of its own. When the first instructions for use of Cipher Device M-138 were published in 1935, 25 alphabet strips were issued in a set with each system. Twenty-five was, of course, the exact number of strips required to fill the 25 channels of the

---

days. For this reason it is necessary to change the sequence from time to time, and the method of determining or indicating the new sequence must be agreed upon in advance and thoroughly understood by all who are to use the instrument.

b. The sequence in which the alphabet disks are assembled upon the shaft constitutes the key in this cipher system. When a change in key is to take place, exactly what the new key will be and the exact moment that it is to supersede the old key will be determined by the proper commander and will be published in signal operation instructions. (For example, see page 272.)"
AS-80A File: Cipher Device M-94.

5. Cipher Device M-94 was later replaced by Converter M-209.

device. These 25 strips were rearranged from time to time and, less frequently, were replaced by a new set of entirely different alphabets. By 1939 a new policy of issuing 50 or 100 alphabet strips in a set was adopted. Since only 25 strips were used in the device at one time, periodic re-selection, within the set of 50 or 100, of the 25 strips to be used, provided more security than rearranging the same 25 strips. From 1939 until middle 1942, the same alphabet set of 50 or 100 strips was frequently in effect for six months.

During the six months in which an alphabet set was effective, the strips were rearranged daily, 25 of the 100 being selected and used. (Period: middle 1939 - middle 1942) However, only 50 different arrangements of the alphabet strips were provided for the entire six-month period, making it impossible to avoid using exactly the same arrangement of the strips on several different days. The method of selection was as follows: Each cipher key list contained two tables. One table consisted of 50 serially numbered numerical sequences, each containing 25 random numbers. Each numerical sequence indicated which 25 strips of the set were to be placed in the 25 channels of the device on a certain day and in what order. (The alphabet strips were serially numbered and each number in the numerical sequence referred to a numbered alphabet strip) Which numerical sequence was used on

Figure 5

SAMPLE KEY TABLE (1939 - 1942)

DAILY KEY TABLE

Note: The key number for a given date is that number which is at the intersection of the column in which the month is located and the row in which the day is located. Example: For April 3, the Key No. is 44.

Day of Month	Month Jan.	Feb.	Mar.	Apr.	May	June	Jul
1	10	38	48	41	1	19	16
2	49	1	23	50	12	29	3
3	22	39	50	44	29	20	6
4	11	12	21	7	9	18	27
5	34	9	8	2	2	24	4
6	1	13	11	40	50	3	36
7	33	32	14	42	35	43	7
8	11	12	10	49	37	4	16
9	39	8	27	38	9	30	8
10	13	1	31	36	15	2	6
11	2	14	26	25	44	3	44
12	24	5	1	6	4	7	8
13	40	28	43	3	22	9	27
14	50	2	49	26	45	48	31
15	41	23	25	21	19	11	9
16	5	29	1	22	8	33	20
17	3	4	34	24	5	21	18
18	42	35	7	45	20	47	25
19	36	33	2	32	3	10	31
20	6	4	34	34	40	41	37
21	37	38	46	35	1	36	4
22	13	1	16	19	2	17	44
23	35	47	39	50	42	4	19
24	11	16	3	33	15	20	32
25	37	32	36	18	40	32	42
26	43	49	10	23	9	5	46
27	12	17	35	18	49	12	31
28	38	15	14	43	24	33	50
29	14		15	46	47	14	18
30	39		48	34	13	43	33
31	16		17		19		20

For further explanation of using this table, see opposite page.

which day was determined by means of a second table. A sample of this second table is given on the opposite page; it was used by finding in the left-hand column the day of the month on which the message was to be sent and next determining, in the proper month column, the key number corresponding to that date. The key number thus found indicated the numerical sequence to be used in arranging the alphabet strips in the device. For example, according to the sample table on the opposite page (Fig. 5), on the 1st day of January, the tenth numerical sequence was to be used; on the second day, the 49th sequence, etc. Note that according to the sample table, the first numerical sequence was to be used on the sixth of January, and also on 2 February, 10 February, 22 February, 12 March, 1 May, and 21 May -- on seven days during the six-month effective period of the alphabet set, the same strips were used in the same identical order. Elimination of the possibility of such repetition began about August 1942 (although it was not eliminated exclusively thereafter) with the introduction of key lists which contained a different numerical sequence, i.e., a different arrangement of the alphabet strips, for each day. After introduction of this type table, its form remained substantially the same throughout the years. An example of such a table appears opposite page 81 (Fig. 6).

Note: The sequence of numbers standing to the right of the column headed "Day of Month" gives the order in which the alphabet strips are to be inserted in the cipher device.

Day of Month	MECHANICAL SEQUENCE														
1	04	27	08	30	05	14	01	11	07	17	16	02	20	29	13	24	03	12	18	06	19	28	09	23	26	22	25	10	21	15
2	23	19	27	29	22	15	06	21	04	16	20	05	17	07	18	02	05	06	10	13	09	14	28	24	12	26	01	25	30	11
3	07	24	30	01	29	15	30	07	25	27	16	11	15	05	26	12	08	04	22	14	18	25	21	06	19	28	02	17	03	10
4	15	11	25	04	24	20	30	21	29	22	25	01	17	07	27	08	13	09	02	14	18	12	10	03	23	05	26	06	19	16
5	15	09	05	20	25	26	17	18	14	07	12	27	21	28	02	11	01	25	06	30	04	19	03	08	15	10	22	16	29	24
6	12	05	19	02	14	06	11	23	21	15	22	25	04	28	15	07	08	20	03	01	30	27	24	26	16	09	18	10	29	17
7	28	11	05	19	09	01	08	13	02	17	20	15	29	26	24	16	05	27	12	21	06	22	25	04	23	10	18	30	14	07
8	24	30	11	28	02	05	07	19	04	09	17	14	22	13	29	26	21	06	23	18	25	01	08	27	30	03	12	16	10	15
9	27	10	19	11	22	15	18	20	02	05	24	09	30	09	13	28	17	08	23	04	06	07	12	28	16	25	21	29	14	01
10	11	30	08	12	06	18	25	24	14	21	05	24	10	28	02	16	07	05	26	09	29	01	13	20	23	15	27	04	19	17
11	19	15	04	08	29	01	18	11	15	27	09	26	23	07	16	05	25	17	25	05	28	20	02	10	21	24	06	30	12	14
12	30	24	07	13	21	05	26	28	15	10	27	02	09	15	19	11	20	23	04	01	29	14	25	12	08	05	06	17	28	16
13	18	29	14	23	06	08	12	19	22	28	05	10	09	15	26	15	07	02	29	01	21	30	11	17	03	16	27	24	04	25
14	26	01	15	25	21	07	22	14	23	29	24	05	19	27	10	06	16	28	04	12	17	05	20	11	08	18	30	02	15	09
15	02	13	29	21	08	10	27	03	06	12	04	16	18	07	09	22	01	29	15	05	26	22	17	15	25	16	24	30	20	19
16	09	18	03	19	04	04	13	01	22	14	30	30	12	17	21	12	10	25	16	30	07	26	12	27	25	29	15	21	08	05
17	13	01	30	06	29	08	23	12	18	03	07	10	05	26	22	11	25	27	23	17	02	04	28	24	20	14	09	19	16	15
18	23	14	20	04	16	25	29	11	06	02	27	15	01	22	09	19	10	12	07	03	30	15	17	08	18	26	28	21	24	09
19	26	02	28	06	14	15	25	19	03	07	12	29	01	17	21	03	25	24	11	04	10	27	16	22	13	30	02	20	18	08
20	12	02	11	20	21	30	17	20	28	08	09	29	18	25	30	29	07	03	16	27	09	03	22	08	15	06	13	01	24	14
21	07	15	04	19	25	30	10	03	16	23	21	16	24	30	09	28	22	06	27	03	20	17	01	26	11	19	12	29	05	02
22	06	30	16	25	04	24	21	29	18	11	29	22	03	17	09	14	23	12	08	03	07	28	01	13	26	15	27	02	29	10
23	13	07	30	03	24	19	08	21	05	22	18	10	20	09	18	04	20	13	13	23	26	02	27	08	29	01	17	10	14	25
24	24	15	22	11	16	20	05	31	01	12	10	06	17	28	03	10	27	02	23	26	09	04	18	07	25	29	14	08	30	19
25	25	28	07	01	21	11	05	03	10	29	22	13	07	18	10	15	23	08	27	30	24	12	19	03	14	20	02	17	26	06
26	04	27	27	16	23	27	13	26	22	08	25	05	10	24	06	21	07	05	29	04	28	13	02	19	20	22	01	18	21	09
27	21	17	14	03	13	03	15	29	11	01	09	25	16	24	06	30	20	25	22	07	28	13	06	26	09	12	19	10	08	27
28	20	16	24	28	30	14	22	10	30	06	08	09	27	25	24	04	17	21	09	19	12	29	07	04	13	16	10	25	01	05
29	22	12	05	11	20	09	15	23	05	25	18	23	25	03	01	16	28	09	29	10	17	14	30	04	24	02	07	21	27	19
30	17	05	27	14	01	25	19	09	05	23	12	26	21	11	01	08	10	06	30	10	15	28	06	29	23	12	27	07	13	26
31	01	22	13	07	24	29	01	03	25	19	14	01	26	06	22	27	09	31	16	16	20	05	15	27	13	21	29	13	09	07

Six month supersession of sets of alphabet strips began to be outmoded about January 1942 when a quarterly and bi-monthly supersession schedule was introduced. Monthly supersession began for some systems in about October 1942. There was no particular date on which quarterly and bi-monthly supersession of alphabet sets, or on which monthly supersession replaced quarterly and bi-monthly supersession. The trend was a gradual one, moving steadily toward decreasing the length of time an alphabet set remained effective. By August 1943, the situation concerning supersession of alphabet sets became static, with monthly supersession of alphabet sets and daily rearrangement of strips within the set.

Although there was no definite date on which monthly supersession of alphabet sets and daily numerical sequences were introduced in all strip systems, there is a significant date -- August 1942 -- when the change was made in many systems. The many changes at this time were the direct result of a security study[6] of System 56 made by the then recently organized Strip Cipher Cryptanalytic Unit, Cryptographic Security Section, "C" Branch, Signal Security Agency.

Although the time element has here been used as the

---

6. For description of this study, see p.91 and footnote 15.

element of comparison, the real element of comparison, as regards security, should be the amount of traffic passed in a system during a given period of time. Naturally, the amount of traffic greatly declined after the war's end. Therefore, the length of time a system remained in effect could be lengthened accordingly without detriment to security. Consequently, after the war, some strip systems were returned to a quarterly supersession basis.

C. Selection of Generatrix

It was recognized from the beginning that encipherment on the same generatrix should be held to a minimum. However, a rule for completely eliminating the possibility of using the same generatrix twice in the same message was not introduced until July 1943. Instructions to the operator on choice of generatrix differed widely through the years. (All of the rules quoted are directed to the operator and apply to encipherment of a single message.)

"Instructions for Using the Cipher Device M-94," published in February 1922, state:

> You must make no record of any kind as to which line above or below the plain text you take for the cipher equivalents.[7]

---

7. This rule underwent a startling reversal in 1943. See quotation on p. 83 from instructions for the year.

Continuation of the rules on selection of generatrix from the 1922 official instructions is as follows:

> Avoid taking for the cipher lines either of the lines immediately above or below the intelligible plain-text line of letters and try to distribute the lines of cipher letters that you do take in a very irregular manner among all the possible horizontal lines at different distances from the plain-text lines. Never make a practice of "favoring," i.e., frequently choosing, a particular line above or below the plain text.

The document, "Instructions for Cipher Device Type M-138" (SIGJOB), published in April 1935; the two documents "Instructions for Cipher Device M-138 and M-138-A" (SIGLOD, published in April 1939, and SIGZOR, published in April 1940); and "Instructions for Using Strip Cipher Devices" (SIGUHR), published in April 1942, all gave the same rule on operator's choice of generatrix:

> Care must be exercised to see that the columns of cipher text chosen are taken in an irregular manner, at different distances from the plain-text columns. However, deliberate attempt should not be made to prevent the selection of columns the same distance from the plain-text column in enciphering a long message. Never make a practice of "favoring," i. e., frequently choosing a particular column to the right or left of the plain-text column. Furthermore, it is to be emphasized that the selection of the columns must never be according to any system or pattern, least of all according to numerical order.

From "Instructions for Using Strip Cipher Devices" (SIGUHR-2), effective in July 1943:

> . . . A note should be made of the interval separating the plain-text column and the selected generatrix. Generatrices selected may be marked with a pencil on the

top of the device and erased later. Generatrices occurring at the same interval from the plain-text column will not be selected more than one time in enciphering a message. Intervals of zero and of twenty-six must never be selected . . .

. . . CARE MUST BE EXERCISED TO SEE THAT THE GENERATRICES TAKEN FOR CIPHER TEXT ARE SELECTED IN AN IRREGULAR MANNER AND AT DIFFERENT DISTANCES FROM THE PLAIN-TEXT COLUMNS. IT IS TO BE EMPHASIZED THAT THE SELECTION OF GENERATRICES MUST NEVER BE ACCORDING TO ANY SYSTEM OR PATTERN, LEAST OF ALL ACCORDING TO NUMERICAL ORDER.

From "Instructions for Using Strip Cipher Devices" (SIGUHR-3), effective in March 1945; and from "Instructions for Using The Strip Cipher Device" (SIGUHR-4), effective in July 1946:

> Always select generatrix numbers in an irregular manner. The selection of generatrix numbers must never be made according to any system or pattern, least of all according to numerical order. Never select the same generatrix number twice in enciphering a message or message part.

D. Message Length Limitation

On 1 July 1943 the first instructions on limitation of length of messages were promulgated by means of the new publication, SIGUHR-2. The rule placed the length limitation[8]

---

8. Message length limitation. - If the cryptographed text of a message will exceed a certain number of groups (100 according to SIGUHR-2; 125 according to SIGUHR-4) divide the plain-text into two or more approximately equal lengths so that no part will exceed the designated number of groups. The two parts are then handled as separate messages.

of messages at 100 5-letter groups. On 1 July 1946 the new instruction document, SIGUHR-4, extended the length limitation of messages to 125 5-letter groups.

E. Channel Elimination

The introduction of the new 30-channel Cipher Device M-138-A was quickly followed by the adoption of a very important security improvement, namely, channel elimination. Next to replacement and rearrangement of alphabets, channel elimination is the most significant addition to cryptographic security. Channel elimination made it more difficult to recognize the use of the same generatrices in different messages by breaking up repetitions in the cipher text.

After the introduction of alphabet strip ciphers, the conception of channel elimination, in some form, seemed a natural inspiration to cryptographically inventive minds; therefore the idea was known from the earliest days of strip ciphers. However, the Army, fearing to confuse its own operators as well as the enemy, hesitated to adopt channel elimination because of its rather complicated nature. When the Navy adopted it, the Army interestedly watched to determine its practicability. In middle 1939 it was introduced in a limited number of Army strip systems.[9] From then on it was gradually

---

9. See pp. 86-89 for detail.

introduced into an increasing number of systems until July 1943 at which time it became the requirement for all systems (Tab 40).

Channel elimination was accomplished as follows:[10] After 30 alphabet strips had been arranged in Cipher Device M-138-A according to the numerical sequence given in the key list, five channels were eliminated from use. In eliminating the five channels, the operator withdrew the strips from the channels and re-inserted them only part of the way in the same

---

10. A procedure which produced the same effect as channel elimination could be used by holders of the 25-channel Cipher Device M-138. The procedure was as follows: (It is quoted directly from "Instructions for Using Strip Cipher Devices," SIGUSA, April 1942.)

(1) Having found in the current Cipher Key List the numerical key for the date of the message, write down this key on a sheet of paper.

(2) Select at random 5 different letters of the alphabet, for example, LEWBA. This group becomes the message indicator and must be shown as the second and next to last group of the cryptogram.

(3) Refer to the channel-elimination table in the Cipher Key List and in the line corresponding to the date of the message find the numbers assigned to the letters of the selected message indicator. For example, assume the values corresponding to the message indicator LEWBA are found to be 5 - 7 - 29 - 6 - 17, respectively.

(4) Now turn to the numerical key already written down, and counting from left to right cross out the 5th, 7th, 29th, 6th, and 17th numbers of the key. The remaining sequence of 25 numbers gives the order and identity of the alphabet strips to be inserted in the device.

(5) The subsequent operations in encipherment will be as in the case of Cipher Device M-138-A.

CHANNEL ELIMINATION NUMBERS (Sample Table)

Day of Month	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Day of Month
1	04	27	08	30	05	14	01	11	07	17	16	02	20	29	13	24	03	12	18	06	19	28	09	23	25	22	1
2	23	19	27	29	22	13	08	21	04	16	20	05	17	07	18	02	03	06	10	13	09	14	28	24	12	26	2
3	09	24	30	01	29	15	20	07	23	27	16	11	13	05	26	12	08	04	22	14	18	25	21	06	19	28	3
4	15	11	23	04	24	20	30	21	29	22	25	01	17	07	27	08	13	09	02	14	18	12	10	03	26	05	4
5	13	09	05	20	23	26	17	18	14	07	12	27	21	28	02	11	01	25	06	30	04	19	03	08	15	10	5
6	12	03	19	02	14	06	11	23	21	13	22	25	04	28	15	07	08	20	05	01	30	27	24	26	16	09	6
7	28	11	03	19	09	01	08	13	02	17	20	15	29	26	24	16	05	27	12	21	06	22	25	04	23	10	7
8	24	20	11	28	02	05	07	19	04	09	17	14	22	13	29	26	21	06	23	18	25	01	08	27	30	03	8
9	27	10	19	11	22	15	18	20	02	03	24	05	30	09	13	26	17	08	25	04	06	07	12	28	16	25	9
10	11	30	08	12	06	18	25	22	14	21	05	24	10	28	02	16	07	05	26	09	29	01	13	20	23	15	10
11	19	15	04	08	29	01	18	11	13	27	09	26	22	07	16	05	25	17	23	03	28	20	02	10	21	24	11
12	30	24	07	13	21	05	26	22	16	10	27	02	09	15	19	11	20	23	04	01	29	14	25	12	08	03	12
13	18	25	14	23	06	08	12	19	22	28	05	10	09	15	20	13	07	02	29	01	21	30	11	17	03	16	13
14	26	01	13	25	21	07	22	14	23	29	24	05	19	27	10	06	16	28	04	12	17	03	20	11	08	18	14
15	02	11	25	21	08	10	27	03	04	12	06	14	18	07	09	28	01	29	13	05	26	22	17	15	23	16	15
16	09	16	03	19	04	02	11	01	22	14	20	30	25	17	24	15	06	18	10	28	07	26	12	27	23	29	16
17	13	01	30	06	29	08	21	12	18	03	07	10	05	26	22	11	25	27	23	17	02	04	28	24	20	14	17
18	23	14	20	04	16	25	29	11	06	02	27	15	01	22	05	19	10	12	07	03	30	13	17	08	18	26	18
19	26	09	28	06	14	15	25	19	03	07	12	29	01	17	21	05	23	24	11	04	10	27	16	22	13	30	19
20	12	02	11	26	21	30	17	20	28	04	29	25	18	23	10	19	07	03	16	27	09	05	22	08	15	06	20
21	07	13	04	19	25	30	10	08	14	23	21	16	24	18	09	28	22	06	27	03	20	17	01	26	11	15	21
22	06	30	10	25	04	24	21	19	18	11	20	22	05	17	09	14	23	12	08	03	07	28	01	13	26	15	22
23	15	07	30	03	24	19	06	21	05	22	12	16	20	09	18	04	28	11	13	23	26	02	27	08	29	01	23
24	24	15	22	11	16	20	05	21	01	12	13	06	17	28	03	10	27	02	23	26	09	04	18	07	25	29	24
25	25	28	07	01	21	11	05	08	16	29	22	13	09	18	30	15	23	04	27	30	24	12	19	03	14	20	25
26	04	17	27	16	23	14	11	30	12	08	15	03	10	26	06	24	07	25	29	05	28	13	02	19	20	22	26
27	21	17	14	03	19	02	15	29	11	01	05	23	16	24	04	30	20	25	22	07	28	13	06	26	09	12	27
28	20	18	24	28	30	11	22	15	26	06	08	03	27	23	14	02	17	21	09	19	12	29	07	04	13	16	28
29	22	13	06	11	20	08	15	12	05	25	18	26	23	03	01	16	28	09	29	10	17	14	30	04	24	02	29
30	17	03	20	14	02	24	18	08	05	23	19	25	22	13	09	08	16	04	30	10	15	28	06	29	22	12	30
31	03	22	18	05	24	30	04	01	25	19	14	02	23	08	17	20	28	11	10	16	20	06	15	27	12	21	31
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

channels but with the reverse sides exposed to view. The specific five channels eliminated varied from message to message on the same day. The method of selecting which five channels were eliminated before enciphering each message was as follows: The operator selected at random, 5 different letters of the alphabet, for example, PLMHO. Next, he referred to the channel elimination table provided in the key list. (See Channel Elimination Table, Fig 7, on opposite page.) In the line corresponding to the date of the message, he found the numbers assigned to the letters he had chosen. Using the table on the opposite page, and the date 16, the letters PLMHO gave the numbers 15, 30, 28, 25, 24. These numbers indicated that the 15th, 30th, 28th, 25th, and 24th channels were not to be used. The numbers in the channel elimination table had no reference whatever to the identifying numbers on the strips themselves. After withdrawing the five strips, the operator enciphered the message by aligning the plain-text letters, 25 at a time, on the remaining 25 strips and then choosing a cipher-text generatrix.

Before 1939 encipherment by means of strip systems was performed with no "interruptor" scheme of encipherment. Twenty-five strips were arranged in the device, the plain-text letters were aligned at the side, and the cipher-text generatrix of 25 letters was chosen. In July 1939 channel elimina-

tion was introduced into two systems, namely, the general CONFIDENTIAL System 26, which was distributed through all levels of command and the general SECRET System 6, also distributed through all levels of command. From that time on, channel elimination was introduced into other systems as considered necessary. In January 1942 a new policy was adopted.

Explanation of the new policy will be deferred for a paragraph in favor of parenthetical remarks concerning the length of time channel elimination tables remained in effect. The sample channel elimination table (Fig. 7, opposite p. 87) shows that a different sequence of channel elimination numbers is given each day. However, only one channel elimination table was included in a key list, meaning that from about July 1939 until early 1942,[11] during which period six-month supersession of key lists was the general rule, the same channel elimination table was in effect. When, from about January 1942 through August 1942, three month supersession of key lists was the general rule, the same channel elimination table was in effect for three months. Beginning about August 1942

11. General statements concerning length of effective periods of key lists can be only approximate because, during the early years 1939 through middle 1942, there was overlapping use of different lengths of effective periods for key lists of different systems. In this case the length of the effective periods of key lists of System 6 has been used.

monthly channel elimination tables were issued with the monthly key lists.

F. Split Generatrix

Beginning in January 1942 channel elimination became the requirement in the encipherment of all SECRET messages. For CONFIDENTIAL messages[12] a new method, known informally through the years as "split generatrix,"[13] was adopted. After 30 alphabet strips had been arranged in the device according to the numerical sequence given in the key list, the operator

---

12. With the introduction of "split generatrix" for CONFIDENTIAL messages, System 56 superseded System 26 as the general CONFIDENTIAL system. Channel elimination had been used with CONFIDENTIAL System 26 but was replaced for CONFIDENTIAL communications by "split generatrix" of CONFIDENTIAL System 56. System 6, with channel elimination, remained the general strip system for SECRET messages.

13. When the 25-channel Cipher Device M-138 was used, the procedure for "split generatrix" was as follows: (The quotation is from "Instruction for Using Strip Cipher Devices" (SIGUHR), April 1942:

> . . . The following procedure is recommended for employment by holders of Cipher Device M-138 whenever 30 channels for sliding strips are required: Insert the first 25 strips in accordance with the numerical key and lay the last 5 strips in key order below the device on the desk or table top. Set up the message according to the instructions for the M-138-A device and the current Cipher Key List for the particular system. Extreme care must be exercised in the alignment of the last 5 strips. Any makeshift, such as slits in the sheet of paper, may be employed to keep them in order. Operating procedure is the same as in the case of Cipher Device M-138-A.

aligned 30 letters of plain-text against the left-hand stop bar. A cipher generatrix was selected at random and the first 15 letters (from the top half of the device) were recorded in 5-letter groups. Next, another generatrix was selected at random and the last 15 letters (from the bottom half of the device) were recorded in 5-letter groups. The recorded letters were the first 30 letters of the cipher-text proper. In no case were all 30 letters ever taken from the same column.

Channel elimination for SECRET messages and "split generatrix" for CONFIDENTIAL messages remained the requirement from January 1942 through July 1943. After the latter date, channel elimination became the requirement, in general, for both SECRET and CONFIDENTIAL messages; however the "split generatrix" was retained in some CONFIDENTIAL systems. At the time of its adoption the belief that the "split generatrix" procedure added security to the general method of using strip cipher systems, was based on early experiments[14] which showed that with generatrices of 30 letters statistical tests could be applied to identify generatrices that were identical. With reduction of the number of letters per generatrix, which was accomplished

---

14. Information concerning the "early experiments" here mentioned was given by Mr. Friedman in answer to the question: "What was the purpose of introducing "split generatrix?" Questionaire containing this question was sent to Mr. Friedman on 14 October 1947.

by the "split generatrix" procedure, this statistical matching was no longer as successful. However, the number of generatrices was doubled thereby, so what was gained in one direction was lost in the other. The split into two generatrices of 15 letters each was practical because of the way in which the strip board was constructed in two equal halves. In early 1943 the ineffectiveness of the "split generatrix" as a security measure was conclusively proved by a security study of System 56, made by the Strip Cipher Cryptanalytic Unit, Cryptographic Section, "C" Branch. This study of System 56, conducted during part of the summer and fall of 1942 and extending into early 1943, took the form of three cryptanalytic tests,[15] the final one of which was successful enough to war-

---

15. The three 1942 cryptanalytic tests of System 56 are summarized as follows:
    a. First test -- No. 7132.1 (Tab 41)
        (1) Given: Messages in complete intercept form. No other information.
        (2) Conclusions: With proper usage, the system had a high degree of security since traffic in the system was unlikely to be heavy enough to give sufficient depth in any one generatrix to allow rapid solution.
    b. Second test -- No. 7132.2 (Tab 41)
        (1) Given: 180 lines of bona fide traffic. 3 plain-text lines of the 180 cipher-text lines.
        (2) Conclusion: The remaining 177 lines were not read in the 6 weeks spent attempting to obtain a solution.
    c. Third test -- No. 7132.3 (Tab 41)
        (1) Given: Various amounts of plain-text for 180 lines of cipher text.
        (2) Conclusions: The problem was successfully

elimination was considered very secure. The system had been tested and retested by the Strip Cipher Cryptanalytic Unit with only negative results. However, in April 1944, the Strip Cipher Cryptanalytic Unit made such significant discoveries that it recommended discontinuing use of strip cipher systems unless some way could be found to substantially improve their security. The cryptanalytic test which brought about this recommendation was as follows: Working with bona fide traffic all enciphered on the same day, the Strip Cipher Cryptanalytic Unit solved the indicator system by a previously unused method.[16a] Solving the indicator system meant that by working with only the indicators (the 5 letters chosen at random by the operator), the cryptanalyst determined the numbers assigned to these letters in the channel elimination table for the day. The extent of the test was that the messages were read and both the thirty alphabets used and the channel elimination table for the day were reconstructed.

On 19 May 1944 a conference was held between representa-

16a. The cryptanalysis was the work of Miss Maxine Devore. The technique used -- as well as many others employed previously -- was original and resulted from independent research and original thinking.

Miss Devore's work had more influence than any other factor in contributing to the shift from strip systems to machine systems.

tives of the Signal Security Agency and representatives of the Navy to discuss strip cipher systems. The Signal Security Agency representative at the conference suggested undertaking a joint study[17] which included a comparison of the security inherent in the Army indicator system. As a result of the study, on 2 September 1944, Army instructions were promulgated[18] changing the Army method of channel elimination to a variation of the Navy method. The Navy procedure for varying the number of channels eliminated was adopted. The variation was produced by two factors: the presence of blanks in the table of strip elimination numbers and the repetition of numbers resulting from the use of five consecutive lines of the table. The Navy method was not adopted completely at this time since the Army method of eliminating strips by channel number instead of strip number was maintained. The Army preferred elimination by channel number because it permitted continued use of 50 or more strips in a set.

The new method of channel elimination, which permitted a variable number of channels eliminated, was accomplished as

---

17. As part of the same study, (a) SSA obtained traffic-load data on all systems used by both the WD and the Theaters; (b) a subcommittee was appointed to attempt to devise a new indicator system.

18. Change No. 2 (2 Sep 44) to "Instructions for Using Strip Cipher Devices," (SIGUHR-2).

Figure 8.

CHANNEL ELIMINATION NUMBERS (Sample Table)

Day of Month	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Day of Month
1	4			1	30	29			10	14			6	18				27	9	24		17	23				1
2	1		13		22		3	24	21		7		20		26	19	5	28			14			23			2
3	26	3		2		17		25		5	16	19	27	10		23	1	22	7	9		18		21		15	3
4	15		13		19		18	28		7	21	2	11			14		25			12		22		29		4
5	19	27	20	10	21	8	23	22	29	24	5	25	2	12	4	6	26	17	11	15	7	28	30	9	3	13	5
6	21		9	24	5	15		27		10		18		28	23	19	25	11		8	20			7	17	1	6
7	3		10	23	11			22		27				19	25	1		8			21		20		6	14	7
8	15	18	17	24	1	27		13		3	11	26			23	29		6		28		21		14	12	22	8
9	28	16	26	27	29	15	4	5	14	23	25	6	22	10	12	20	30	18	1	21	17	11	7	3	9	2	9
10		1		22			24				11	10	30	19	6			2	4	25		5		13			10
11	6	14	29	8	9	17		4	18	23	21			20			22		2	24			28	26			11
12		23	17	24		1	20	28	2		30		25	16			27	6	8		3	10			14	18	12
13	1	3	27	26	16	9	12	30	19	25	29	8	5	15	21	14	6	23	10	4	7	2	22	28	13	17	13
14		30		9		23	17	2	15			25			6		14	22	5			16		24	20	8	14
15	22		4		28		8			11	17			20			26	7	23	27	14	5	19	16		9	15
16	7	22	16	11	10	17	23	12	30	15	18	9	3	19	20	2	14	4	13	29	25	24	27	5	21	1	16
17	15	30	19	4		9	25	29	20	5		12	24	2				16	22	26		21				10	17
18	18				9	10	7	15		3		28	25		17	29	23	24	16	20			11		12			18
19	12	24	22		27		19	11	17	16	13	8		3	28	18		5	14		26			9			19
20	28	3	15	6	30	26	25	1	18	2	11	5	7	10	21	27	4	14	20	29	17	16	19	8	25	12	20
21	13	23	10			14		30			20	11	25	15								22	27	28	2	8	21
22	8					16		11	28		9	21			5	20		4	2		12		26	3			22
23	12			13				17	10		18	14		21	19	23	11			9		4		29		3	23
24	18	22	29		13	30	23	27				17	4		2	5	19			12		8		26	7		24
25	13	4	26	1	22	17	19	10	11	21	23	8	24	2	27	9	6	15	16	29	5	30	28	3	20	7	25
26	22		20	21		4		12		5	28		17		15			3	1		8		2		9	6	26
27	26	7	9	6	21	5	25	8	17	27	18	30	12	22	11	1	16	23	19	4	3	13	20	10	15	29	27
28	28	18	24	11	10	30	27	29			6	13		5	3			21	1		14		26			20	28
29			6	8	9			26			10		27	14	11		4	16	13	23	29			18	28		29
30	10	27			15	26	23		30	1		20	17	21		8	13	19		11	4	29		2	22		30
31	15	5	10	29	13	19	30	2	17	28	27	4	8	25	20	14	7	9	16	18	3	23	12	11	21	26	31
32			17				22	8	2	21	29		30			23	13	19	12					6		7	32
33			4	7				27	22		12		3	10		16	30	26		1		2	28	17	19	20	33
34		11	15	19	26			18			25			23					21	7	22	13		8		3	34
35	26	4	1	29	21	2	28	3	18	22	9	15	11	12	6	16	8	27	30	13	24	20	23	10	7	19	35
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

follows:

First, the operator selected at random five different letters of the alphabets. Second, he then referred to the current channel elimination table (See the sample table, Fig. 8, on the opposite page).[19] Third, he then found in the line corresponding to the date of the message, the number which was in the column designated by the first letter of the 5-letter group chosen by the operator. Next, in the line immediately below the current date line, the operator found the number appearing under the second letter of the 5-letter group chosen, etc. until a number for each letter of the 5-letter group had been found in successive lines of the channel elimination table. The instructions[20] contained the following precaution:

> Do not attempt to change an indicator which eliminates fewer than five channels to one which will eliminate five channels. The variation in the number of channels eliminated increases the security of the system.

An example of the procedure for varying the number of

---

19. There were 35 sequences in this table instead of the 31 sequences of the previously used table (opposite p. 87). The last four lines of the new-type table were required because five successive lines of the table were used to determine which channels were to be eliminated; on the thirty-first of the month, for instance, lines 31 to 35 were used.

20. "Instructions for Using Strip Cipher Devices," (SIGUM-3) effective 1 March 1945.

channels eliminated follows:

Assume LBKGN to be the 5-letter group chosen by the operator, 29 August to be the date of the message, and the table opposite page 95 to be the table of channel elimination numbers currently in use. Line 29 (corresponding to the date of the message) shows a blank under L, indicating to the operator that no channel would have been eliminated by the first letter of the 5-letter group. In line 30 (the line immediately below the date line) the number 27 appears below B, the second letter of the 5-letter group; therefore the operator would have eliminated the 27th channel. In line 31, the number 27 appears below K, the third letter of the 5-letter group. Since the 27th channel had already been eliminated, the operator disregarded the number 27, as indicated here. In line 32, the number 22 appears below G, the fourth letter of the 5-letter group; therefore, the operator eliminated the twenty-second channel. In line 33, the number 10 appears below N, the fifth letter of the indicator; therefore the operator eliminated the 10th channel. The numbers derived from the sample 5-letter group chosen by the operator consisted of the three numbers -- 27, 22, and 10. Therefore, only three channels -- the 27th, 22nd, and 10th -- were eliminated.

H. Change from Channel Elimination to Strip Elimination

The method of channel elimination described in the para-

graph above prevailed until 1 July 1946 when instructions requiring elimination by strip number instead of channel number were promulgated.[21] The difference is simply that the five numbers, from the elimination table, designated by the 5-letter operator-chosen group, refer to the strip numbers and NOT to the channel numbers. For example, if the five numbers designated by the 5-letter operator-chosen group are found to be 27, 27, 20, 22, --[22] these numbers refer to strip number 27, strip number 20, and strip number 22 instead of channel number 27, channel number 20, and channel number 22. This new factor brings about reversed warnings on this point. The document "Instructions for Using Strip Cipher Devices" (SIGUHR-3), effective 1 March 1945, contains the italicized directive in reference to the channel elimination table of the cipher key list:

> The numbers in the sequences refer to the channels of the device and have no reference whatever to the strip numbers.

"Instructions for Using The Strip Cipher Device" (SIGUHR-4), effective 1 July 1946, contains the reverse directive:

> The numbers in the sequence refer to the strip numbers on the right of the alphabet strips.

---

21. The reasons for these changes are given on pp.99-104.

22. As before, the repetition of a number and the appearance of a blank means that only three strips are to be eliminated.

Two other changes which came about at the same time, 1 July 1946, are significant. The first, which is directly contingent upon the change from channel elimination to strip elimination, is that 50 or 100 strips in a set could no longer be the number of strips issued. The new policy was to issue, with each system, 30 strips of one color for encipherment of SECRET messages and 30 of another color for messages of lower classification.[23] The other change concerned the 5 letters, chosen at random by the operator, which designated 5 numbers in the elimination table. All directives on this point in the instructional material issued prior to SIGUHR-4, effective 1 July 1946, require that the operator choose, at random, 5 different letters. "Instructions for Using The Strip Cipher Device" (SIGUHR-4), 1 July 1946, permitted repetition of

---

23. The following is a quotation from paragraph 2a, Memo for the Chief, ASA; From Ass't. Chief of Staff, G-2,30 Oct 45:
> . . . Each strip cipher system should consist of necessary keying data and a set of 60 strips; 30 strips to be one color and employed in the encipherment of secret messages; 30 to be of another color. The Navy should use the latter set of strips for confidential and restricted traffic, the Army for confidential messages only (the Army will continue to use its world-wide strip cipher system for restricted traffic, this system to consist of a set of 30 strips).

The world-wide strip cipher system for Army RESTRICTED traffic was System 999, which was discontinued 1 Jan 47. After this date the new policy was the same as the Navy's, namely, the second group of strips was used for CONFIDENTIAL and RESTRICTED messages.

letters in the 5-letter operator-chosen groups. The new rule is quoted as follows:

> . . . Select at random any five letters of the alphabet. Repetitions of individual letters are permissible if they occur by chance . . .

The above described changes concerning or contingent upon strip elimination, which became effective 1 July 1946, reached consummation as part of a tremendous project instigated by the Joint Communications Board. At its meeting on 20 June 1945 the Joint Communications Board appointed an AD HOC committee on Security of Communications. It was composed of Army and Navy representatives of the Joint Security and Joint Methods and Procedures Committees. The main purpose of this AD HOC committee was to

> undertake a survey to determine whether the basic doctrine governing classified communications, and specific fules, regulations, methods, procedures, and practices provide the highest degree of communications security compatible with operational requirements.[24]

This survey was limited to U. S. Army, U. S. Navy, and U.S. Joint Communications, but included consideration of those aspects of combined communications which might be involved in the survey of U. S. intra-service and U. S. Joint communications. The report of this survey was to be submitted to the Joint Communications Board as soon as practicable.

---

24. Quoted from the JCB Directive to the AD HOC Committee on Security of Communications.

Now a question is raised: Why did the Joint Communications Board consider it necessary to undertake such a project at this particular time? The answer is found in the fact that upon the return, about February 1945, of Rear Admiral J. R. Redman and Captain J. W. Wenger of the Navy from a world trip and the return of Major Clapp of the Army from an inspection tour of the European Theater, all three officers reported divergencies in communication practices which led to confusion and delay. The findings of these three officers were reported to the Joint Security Committee which, in turn, recommended that the Joint Communications Board appoint an AD HOC committee to conduct a survey of the security of Allied Communications. The appointment of the AD HOC Committee on Security of Communications, discussed in the paragraph immediately above, was the direct result of this recommendation. At the first meeting of the AD HOC Committee on Security of Communications, the members decided that the committee would conduct the above survey by means of five subcommittees or "working" committees. The working committees were as follows: (1) Committee to survey Call Signs and Delivery Groups, (2) Committee to survey Codes and Ciphers, (3) Committee to survey Frequencies and Circuits, (4) Committee to survey Procedures in Message Headings, (5) Committee to survey Certain Specific Aspects of Security. The five committees are listed here to show the

range of the project undertaken and, thus, the relation of the new policy concerning strip ciphers to the whole project of resolving divergencies in Army and Navy communication practices.

The committee which was directly responsible for the changes concerning strip cipher systems was the "working" committee on Codes and Ciphers. The report[25] of this committee formed a part of the total report of the AD HOC Committee to the Joint Communications Board; the part of the report which is particularly pertinent follows:

> It can be demonstrated that a continuing potential source of insecurity of codes and ciphers is the fact that while the Army and Navy employ, in many cases, the same basic systems (e.g., strip cipher, ECM-SIGABA), there are differences in service rule as to the methods of use of the systems. It might be considered axiomatic that where two methods exist for the employment of a cryptographic aid, one must provide a higher degree of security than another. This is probably true with the

---

25. The report on the "working" committee on Codes and Ciphers which formed a part of the total report of the AD HOC Committee on Security of Communications contained the following remarks which directly concerned strip cipher systems:

> e. The strip cipher has provided an acceptable degree of security when strip (channel) elimination is employed. In view of its security limitations, however, it is not suitable for continued use as a primary general purpose cryptographic system, although it has definite advantages as a stand-by system in view of its simplicity and ease of stowage.
>
> f. In considering cryptographic systems for future adoptions those systems which by their inherent characteristics facilitate the fitting of cribs (e.g., flat strip cipher, enigma-type cipher) should be avoided.

exception that in some cases service requirements may tend to balance out such inequalities of security. Where differences do exist, it has been found necessary to adopt the procedure of one or the other of the services for Joint systems, each service continuing to employ its own procedures for intra-service use. Such a situation is detrimental to security in that cryptographic personnel must learn two sets of rules and methods, and may inadvertently employ (and have done so) intra-service rules to Joint systems.

Through channels the above series of events resulted in the following G-2 directive which effected the new regulations for strip cipher systems:

WAR DEPARTMENT
WAR DEPARTMENT GENERAL STAFF
MILITARY INTELLIGENCE DIVISION, G-2
WASHINGTON 25, D.C.

MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Joint Policy and Procedures Governing the Use of Strip Cipher Systems

1. The Joint Communications Board has considered the difference in Army and Navy procedures regarding the use of strip cipher systems, and the effect upon the security of Army, Navy, and Joint Communications.

2. The Joint Communications Board has adopted the following long-range policy concerning the use of strip cipher systems:

a. Wherever and whenever possible strip cipher systems should be removed from regular use.

b. Strip cipher systems should, in every case possible, be relegated to the position of back-up, or emergency, systems.

c. The Army and the Navy should take necessary steps to develop a cryptographic device to replace strip cipher systems as regular systems in those

instances where cipher machines already developed cannot be used.

3. The Joint Communications Board has adopted the following procedures concerning the use of strip cipher systems in cases where such systems must still be used. These procedures should become effective as soon as production methods can be changed and necessary amendments to existing instructional documents can be promulgated.

a. Each strip cipher system should consist of necessary keying data and a set of 60 strips; 30 strips to be one color and employed in the encipherment of secret messages; 30 to be another color. The Navy should use the latter set of strips for confidential and restricted traffic, the Army for confidential messages only (the Army will continue to use its world-wide strip cipher system for restricted traffic, this system to consist of a set of 30 strips).

b. All elimination of strips should be "strip" elimination, wherein the numbers of the elimination table will designate the numbers of the strips to be eliminated and not the channels from which the strips are to be eliminated.

c. The permitted length of a cryptographic part should be 125 groups.

4. It is desired that the above policy be adopted for intra-Army use and appropriate instructions issued pertaining to the use of strip cipher systems.

FOR: CLAYTON BISSEL
Major General, GSC
Asst Chief of Staff G-2

/s/ R. C. JACOBSON
Colonel, GSC
Actg Deputy

Only the security studies which affected major changes in use of alphabet strip systems are mentioned in the text of this history; however, the Strip Cipher Cryptanalytic Unit has

compiled a detailed report of all its security studies. A detailed list of these studies is given in Tab 41. The security studies listed in Tab 41 appear in two volumes, entitled "STRIPS, Volume I" and "STRIPS, Volume II". These volumes are available in Analysis Section, Methods Branch, Security Division, Army Security Agency.

There is also available now from TICOM studies information on German and Japanese cryptanalysis on Army and State Department strip systems. The most successful work was achieved by the Cryptanalytic Section (Pers ZS) of the German Foreign Office, which read our diplomatic strip traffic until sometime in 1944. During this period the State Department was using the "split generatrix" procedure.[26] After channel elimination was adopted, German cryptanalytic success appears to have ceased. From all available information, Japanese success on our diplomatic traffic appears to have been confined to physical compromise only. In the Army systems German cryptanalysis appears to have been successful only on the traffic enciphered with Cipher Device M-94.[27]

---

26. See pp. 89-92.

27. See Chapter II, pp. 22-26.

CHAPTER X. UNADOPTED PROPOSALS FOR MODIFICATION OF CIPHER DEVICE M-94, M-138, M-138-A

Mr. William F. Friedman proposed, through the years, several unadopted modifications for increasing the security of the strip device for which he holds the patent. He also proposed an unadopted modification of Cipher Device M-94.

The proposal for modifying Cipher Device M-94 (offered in July 1929) contemplated a change from 25 disks to 25 sliding strips; these strips, instead of being flat, were to be square prisms of brass, wood, bakelite or some similar material. Each side or face of the prism was to bear a mixed alphabet, all alphabets to be different, thus making the 25 prisms equivalent to a set of 100 single-alphabet strips. A numerical sequence derived from a key word was to be used to arrange the prisms. The "side up" on each prism was to be indicated by a subsidiary indicator developed from the same key word or by some other suitable method. More details concerning this proposal are given in the Security Reports on Strips, Vol. I, Report No. 7121.1, Security Division, Methods Branch, Analysis Section, Literal Systems Subsection.

In early 1936 Mr. Friedman disclosed a proposal which he developed for a modification of Cipher Device M-138. This modification was to take the form of a sectional device, the sections of which could be rearranged. Mr. Friedman told

Lieutenant J. W. Wenger of the Navy, in Mr. Frank B. Rowlett's presence, about his idea for modification. Mr. Friedman's report of his disclosure to Lieutenant Wenger and the comments which followed are quoted:

March 9, 1936

MEMORANDUM ON CIPHER DEVICE TYPE M-138

This morning I disclosed to Lieutenant Wenger, Code and Signal Section, Navy Department, my idea for a modification of the Strip Cipher Device as follows:

Arrange the device to consist of serially numbered sections of five channels each. To set up the numerical key for the day arrange the sections in serial order from 1 to 5 and insert the individual alphabets in the successive channels in accordance with the daily numerical key. Each message would begin with an indicator which would indicate arbitrarily the order in which the section were to be assembled. This would afford 120 different sectional arrangements.

We commented upon this scheme with Mr. Rowlett being present. During the course of the discussion the question came up as to weakness introduced by the fact that the sections were always of the same number of alphabets, in this case, five. During the course of the discussion I brought up the matter of the Treasury Department Device with its 30 alphabets, and noted that one of the objections to it was that while we had found it extremely difficult to match lines containing 25 letters by means of statistics based upon coincidences, it might be that with 30 letters, which gives 20% more text, the matching of lines to determine which were in the same generatrix might be much easier. I then went on to say that with an arrangement such as I proposed that if the sections were interchangeable this objection to a 30-alphabet device would be eliminated and from that point on I suggested that one might have six sections of which only five would be selected according to the indicator. Continuing I said that I had given some thought to a device in which one could easily vary the number of alphabets in each section, but that I had not arrived at a practicable solution mechanically.

sections themselves of unequal widths. Then I said, for example, supposing that Section 1 had 3 alphabets, Section 2, 8 alphabets, Section 3, 4 alphabets, Section 4, 1 alphabet and Section 5, 9 alphabets, totaling 25 alphabets, the message indicator would indicate the arrangement of these sections for each message so that each message would have 25 alphabets but arranged in different sections. I then said something about the packing of the sections in transporting of the different widths of the sections. Mr. Rowlett pointed out that if one had six sections varying in widths from 4 to 9 alphabets, this would afford a total of 39 alphabets available of which an individual message would use 30 to 35 alphabets depending upon the indicator. At the same time this would combine the advantages of the 30 alphabet arrangement which affords 720 different arrangements of six sections.

Lieutenant Wenger said that he would give the proposal some thought and would talk it over with his associates. He stated that it seemed to him to have good possibilities.

/s/ William F. Friedman

I was present at the above-mentioned conversation and, to my knowledge, the statements made in this memorandum are correct.

Frank B. Rowlett

In 1943 a proposal was made to modify the printing of the alphabet strips in order to decrease the length of cipher text by enciphering figures without spelling them out. The originator of this proposal is not known. The appearance and operation of the proposed modification was to be as follows:

A. Appearance

1 - Each strip to be printed with the same space allowed for letters as on the usual alphabet strip, but with the letters printed in black occupying only the upper half of the strip.

2 - The lower half of each strip to contain the following items printed in red or another contrasting color, in vertical alignment with

the letters and in random order:

a - digits 0 through 9
b - decimal point (.)
c - dash (--)
d - slant (/)
e - first and second parentheses (( ); ( )).
f - comma (,)
g - symbol to represent the "figures-letters shift"
h - symbol to represent "repeat"

B. Operation. The strips are operated as in the usual manner with the following exceptions:

1 - The "figures-letters shift," enciphered in the normal manner, is inserted when a shift from letters to figures or from figures to letters is made.

2 - Each group of figures with accompanying punctuation is repeated with the "repeat" symbol inserted between repetitions. Example: May 10, 1943, prepared for enciphering, would read as follows:

figures MAY letters shift 10 repeat 10, 1943 figures letters shift

3 - Punctuation marks are used only with figures and are not used in punctuation of sentences.

This proposed modification was tested by the Analysis Section, Methods Branch, Security Division, for practicality. The conclusions were that the disadvantages of the proposed revision so far outweighed the slight advantages of shorter messages that it was considered impractical for military use.

In early 1944 Mr. Friedman sponsored a proposal for revision of Cipher Device M-138-A. This revision was to con-

sist of a grille which could be laid over the channels of SIGWOWO, thus providing a method of taking every cipher-text letter from a different generatrix. Several types of grilles were constructed and various methods for using them devised. Details on the grille modification are filed in AS-80A File: Attachment for Cipher Device M-138-A.

CHAPTER XI. ISSUE OF STRIP SYSTEMS TO HOLDERS OUTSIDE THE UNITED STATES ARMY

The Army Security Agency has never had authority to issue cryptosystems outside the U. S. Army. This responsibility rests with the Director of Intelligence. However, the Army Security Agency has had some share in this function. Usually the need or request for issuing cryptomaterial came first to the attention of the Army Security Agency either through the Signal Corps, the Chief Signal Officer, or from ASA personnel in the field. The Agency would then, in each specific case, present pertinent background material and other information to the Director of Intelligence and recommend what action should be taken. Then, if authorization was approved, the Agency prepared and distributed the proper cryptomaterial. (Tab 42).

A. U. S. Government Non-Military Organizations

Many U. S. Government non-military organizations found it necessary during World War II to make use of cryptographic systems in order to safeguard classified information. When regular commercial lines of communication were used, the cryptosystems were provided either by the Army Security Agency[1] or by the

---

1. In each case issuance was authorized by the D/I. See ltr 11 Nov 42 from TAG to CSigO (File AG 400 (11-6-42) OB-S-B) in which the statement is made that issue of cryptomaterial "to any agency of the Federal Government, including the War Department, will be cleared through the Special Branch, Military Intelligence Service." (See Dist & Acct for Cryptomaterial, Central Files, AS-80.).

Office of Naval Communications. The particular type of cryptosystem made available to U. S. Government non-military organizations depended upon (1) the communication facilities to be used, (2) the amount of traffic involved, (3) classification of the information transmitted, (4) number of holders involved, and (5) the availability of the cryptomaterial. Strip systems were issued whenever possible because (1) they were easy to use, (2) they required little storage space, (3) they required no maintenance by military personnel, (4) the security they provided was adequate, and (5) the material required was readily available.

Among the U. S. Government non-military organizations (see Tab 43) supplied with strip systems by the Army Security Agency were the following:

1. Civil Aeronautics Administration.
2. Department of the Interior, Division of Territorial and Island Possessions.
3. Federal Communications Commission.
4. Foreign Liquidation Commission.
5. The Manhattan Project.[2]
6. Office of Scientific Research and Development.
7. Office of Strategic Services.
8. Office of War Information.
9. Panama Canal Office.
10. Rubber Development Corporation.
11. State Department.

At the end of the war many of these U. S. Government non-military agencies were dissolved because there was no further

---

2. During the war the Manhattan Project was a military organization - afterwards it became a civilian organization.

demand for their services. However, other non-military agencies from time to time still required cryptomaterial and strip systems, among other items, were issued to these agencies

B. Foreign Governments

When systems were issued for the use of the armed forces of other governments, strip systems were, as a rule, the type supplied.[3] All requests but one[4] from foreign governments in World War II for cryptosystems came from our own Army personnel who had to maintain secure communications with personnel or units of a foreign country in a specific communication situation. (See Tab 44).

In World War II special authorization was obtained for issuance of Army strip systems to Army units of the foreign countries listed below.

Brazil: "Instructions for Using Strip Cipher Devices" (SIGUHR) was translated and alphabet strips were prepared and issued to the Brazilian Expeditionary Forces.[5]

---

3. For other cryptosystems supplied to Foreign Governments see Volume VI, Command, Coordination, and Liaison.

4. Costa Rica p. 113.

5. This information is contained in a report entitled "The U. S. Cryptographic Contribution of Other Countries," Folder: "Cryptographic Systems Held by Foreign Governments," in files of AS-80A. No further documentation can be found at present, and this reference cannot be confirmed.

Canada: On 14 January 1944 the Director of Intelligence sent to the Chief Signal Officer his approval for the issuance of "Instructions for Using Strip Cipher Devices" (SIGUHR-2), to the Canadian holders of strip systems 1725 and 1745.[6]

In early 1948 issuance of "Instructions for Using the Strip Cipher Device" (SIGUHR-4)[7] was made by 752d Air Force Base Unit (122d AACS Loran Liaison Unit) to Royal Canadian Air Force units at Edmonton, Alberta; Fort Nelson and Dawson Creek, British Columbia; Gimli, Manitoba; and Hamlin, Saskatchewan. These RCAF units, along with certain USAF units, were engaged in a joint project requiring the transmission of classified messages.

Costa Rica: On 24 April 1944 the United States Military Mission to Costa Rica, while making extensive recommendations for the reorganization of the Costa Rican Army along modern lines, asked G-2 for permission to provide certain elementary cryptosystems for use in the reorganized Costa Rican Army.[8] It was believed undesirable at this time to furnish information

---

6. Folder: "Cryptographic Systems Held by Foreign Governments."

7. For method of use prescribed in SIGUHR-4, see Tab 39.

8. See Tab 45. A discussion of policy as to why France and Italy could be issued strip systems while Costa Rica could not may be found in Volume VI, Command, Coordination, and Liaison.

concerning current U. S. Army systems to Costa Rica. However, since Cipher Device M-94 was obsolete[9] and information concerning the device had been disseminated for years in FM 24-5, Signal Communications, it was decided "no threat to security would arise as a result of providing the Costa Rican Government with information and instructional material on the M-94." A copy of FM 24-5, Signal Communication, was forwarded to the Chief of the U. S. Military Mission to Costa Rica.[10]

France: On 28 August 1943 a message arrived from AFHQ announcing the possibility of an early assignment of a French Corps, consisting of two infantry divisions, to the United States Army Command in AFHQ and requesting that proper approval be obtained and cryptographic material be prepared and forwarded for arrival at AFHQ before October 5. On 3 September 1943 the Army Security Agency sent an explanatory letter to the Director of Intelligence requesting authorization to issue strip and Converter M-209 systems to the French. This authorization was granted on 4 September 1943, and in accordance with it two editions of strip System 497 (SIGNGS) were produced on 6 September 1943. A French translation of the document "Instructions for Using Strip Cipher Devices" (SIGUHR-2) was also

---

9. See chapter II, p. 25.

10. The device itself was not furnished, but the FM contained a description of the device and explained its operation.

provided (see Tab 46).

The French were again supplied with a strip system in early 1945. Between 12 and 18 December 1944 seventeen editions of System 465 (SIGAMO) were produced. The system became effective on 1 May 1945[11] and was discontinued in December[12] of the same year.

Great Britain: The Combined Cipher Machine (CCM), was developed and used by the U. S. Army, the U. S. Navy, and the British Services. In line with the normal policy of providing safeguards against interruption of communications through compromises, the CCM was provided with a stand-by system[13] of strips.

The records are confusing in respect to the exact number of strips and strip boards issued by the United States to the United Kingdom. The Minutes of the Combined Communications Board show an early estimate was made by the British of their requirements and they thought that 1,000 copies of the alphabet strip would suffice for their needs. This estimate was later revised upwards to 2,533 copies. No mention is made in

---

11. I.O.M. 258, 23 Apr 45, Information and Records Section, Security Division.

12. I.O.M. 360, 18 Dec 45, Information and Records Section, Security Division.

13. See chapter VIII, p. 70.

the estimate of the number of strip boards that would be required.[14]

The Minutes of the Combined Communications Board (CCB) dated 15 November 1944 state the British reported that only 700 of the 1,600 cipher devices requested had been delivered to the United Kingdom. However, one of the members of the CCB declared he had checked the distribution account records and that 860 of the devices had been delivered to the United Kingdom over a long period of time. This disparity of figures is made more confusing by the fact that the CCB Minutes of some four months earlier (17 May 1944) state "a total of 1,150 [devices] had been sent to the United Kindgom up to that time." Later, on 10 January 1945, the minutes show that an additional 2,165 CSP 845 (Plastic) devices were sent to the Admiralty.[15]

---

14. Ltr 25 May 43, British Joint Staff Mission to OCSigO, and Minutes of CCB, 28 Jul 43. Folder CCBP 0124, 0125, 0126, A3-82 files. The breakdown of the distribution of strips asked for by the British on 28 Jul 43 was as follows:

Royal Navy	1,000
Army	950
Royal Air Force	400
Dept Natl Def - Canada	20
Reg Pub Sect - Aust	50
RAAF Representative	50
Aust Mil Mission	50
Aust Legation	3
British CCB	10
	2,533

15. See Chapter VII, p. 65.

Italy: On 4 November 1943, approximately three weeks after Italy joined the United Nations as an ally, the Director of Intelligence granted authorization to the Signal Security Agency to produce and issue to AFHQ the following cryptographic material for distribution to units of the Italian Army and Air Forces fighting under the U. S. Fifth Army: (1) the instructions for operating strip systems, (2) either the strip cipher device CSP 845 or SIGWOW0, and (3) special alphabet strips and key lists. AFHQ, which originated the request, translated SIGUHR-2[19] into Italian while awaiting approval for issuance of the material. Approval was given 4 November 1943 and the material issued to Italian Army Units.[20] (See Tab 47).

---

18. Ibid.

19. SIGUHR-2 required channel elimination but did not provide the later adopted and more secure instructions for varying the number of channels eliminated. Whether or not the Italian units used strip systems after the new method was adopted in September 1944 is unknown.

20. Confirmation from Curtis Wernl who was in the section (of 849th Signal Intelligence Service, AFHQ) which issued the material.

Philippine Army: Access of properly authorized personnel of the Philippine Army to Cipher Devices CSP 845 and M-138-A and associated alphabet strips and key lists was authorized in February 1945. However, personnel of the Philippine Army could use the devices or have access only to those associated key lists and documents which pertained to cryptographic systems specifically designated for use within the Philippine Army or between elements of the Philippine Army and the United States Army or Navy.

In accordance with this authorization, several strip systems were locally issued to the Philippine Army for operational use.[21] (See Tab 48).

USSR: Seven[22] different cryptosystems were authorized for joint use between the Union of Soviet Socialist Republics and the United States. These were:

1. Strip.
2. M-209.
3. One-Time Pad.
4. Subtractor Tables for Meteorological Systems.
5. Ground/Air Weather. [ALACO]
6. Authentication Systems.
7. Double Transpoeition.

Of the above systems there were only two occasions when strips were involved. The first was System 204 (SIGDBI), which

---

21. Ltr HQ SWPA, 28 Feb 45, file CCBP Folder. Verbal confirmation of this fact from Thomas R. Chittenden, 17 Jun 48. Mr. Chittenden remembers that when he was in the Philippines such material was actually issued.

22. See Tab 49.

was given to the Russians in 1943.[23] The basic document "Instructions for Using the Strip Cipher Devices" (SIGUER), after certain deletions, namely, the section on channel elimination, was translated into Russian.[24] The instructional document at that time[25] required channel elimination for SECRET messages but the more secure method of varying the number of eliminated channels had not been adopted. For CONFIDENTIAL messages the "Split generatrix" was used.[26]

Although authorization from G-2 for issuance of Strip

---

23. Record cards in AS-82 for System 204 show the following:
"DBI Nos 101 thru 106
DBI-5 Nos 101 thru 104, 106 and 107
Transferred to Russians by General Bradley. Removed from accountability on 26 Jan 44."

24. A memo from Mr. Friedman on this subject contains the following remarks:
"My recollection is very clear that we had at least one meeting here with a Russian Army Captain who was to arrange for communications relative to General Deane's mission -- their journey from U. S. to Moscow via Far East. I sat in that meeting, early in 1942 (we were still in the Munitions Building, I think) with Earle Cook and we showed the Russian a device, also how to use it, etc. The instructions were to be translated into Russian."
Mr. Vernon E. Cooley, (then 1st Lt. S. C., OIC of the Code Compilation Unit in 1942) says he also remembers the SIGUHR translation. The section on channel elimination had been included by accident and only at the last moment was this fact noticed. It was then necessary to work overtime typing new stencils and deleting all reference to channel elimination.

25. See Tab 39.

26. See Tab 39.

System 204 to the Russians must have been secured, no record of this approval can be found at this time (December 1948). There is record of authorization for a different system, for on 26 January 1944 the Director of Intelligence approved the issue, when necessary, of strip systems and six other types of systems to the Russian Armed Forces.[27] The list of systems approved at this time was drawn up by the Signal Security Agency for the Chief Signal Officer in compliance with a directive from the Joint Communications Board dated 30 December 1943.

The second strip system prepared for Russian use was never issued. In response to a request from the Signal Intelligence Division, United States Forces, European Theater, strip material was sent to USFET in September 1945 for the purpose of joint communication between Russian and American units in the Allied occupation zones of Europe. The "Instructions for Using Strip Cipher Devices" (SIGUHR-3) was translated into Russian and given the short title SIGWHUT-1. Stencils for use as master copy in the production of monthly key lists were also made up. The only change in context between the two documents was deletion of reference to the wooden strip board SIGWOWO, and the M-138-A aluminum board, and changing "devices" wherever it appeared in SIGUHR-3 to "device." SIGUHR-3 contained the new

---

27. See Tab 49.

method of channel elimination.[28] The system was sent to European Theater Headquarters on 18 September 1945. More than a year later, on 16 October 1946, the Army Security Agency sent a message to USFET to inquire as to the status of the Russian strip material. On 26 October 1946 an answer was received stating that the system had never been distributed to the Russians. The Theater was then directed by the Army Security Agency to destroy the material.[29] The reason why the system was not used is unknown. At the time the material was being prepared for Russian use an interesting letter, dated 18 August 1945, was written by the Assistant Director of Communications Research[30] to the Chief, Army Security Agency. (see Tab 50) which indicates that the policy-makers of the Agency were not in complete accord in regard to the question of providing our Allies with our own cryptosystems for joint use. This is shown in the following quotation from the letter:

> . . . The furnishing of such systems [the reference is to the strip material being prepared at that time for Russian units] seems to be in line with previous policy of furnishing the French and other Allies with U. S. systems for joint use. I have always questioned this policy and would prefer to see the others furnish their systems to us after first making the necessary security changes. In the present case I think it especially undesirable to furnish a U. S. system.

---

28. See Chapter IX, p. 94.

29. Destruction report received at ASA 30 Jan 47.

30. Mark Rhoads, Captain USR (Retired).

Photo No 3

3d page of ~~[illegible]~~ Tab 1 (Hist of Strip Cipher Device)

Now the cylinder of wheels is fixed with the jumbled alphabets on their peripheries, by only changing the order of the wheels in the cylinder an immense variety of different cyphers may be produced for different correspondents; for whatever be the number of wheels, if you take all the natural numbers from [unity] to that inclusive, & multiply them successively into one another, their prod[uct] will be the number of different combinations of which the wheels are s[us]ceptible, & consequently of the different cyphers they may form for diff[erent] correspondents, entirely unintelligible to each other. for tho' every one posses[s] the cylinder, and with the alphabets similarly arranged on the wheels, yet if [the] order be interverted, but ~~one~~ one series similar ~~line~~ through the whole cylinder can b[e] produced on any two of them.

a.b.c / a.c.b / b.a.c / b.c.a / c.a.b / c.b.a

e.a.b.c.d / e.a.b.d.c / e.a.c.b.d / e.a.c.d.b / e.a.d.b.c / e.a.d.c.b — 6
e.b.a.c.d / e.b.a.d.c / e.b.c.a.d / e.b.c.d.a / e.b.d.a.c / e.b.d.c.a — 6
e.c. &c — 6
e.d. &c — 6
24

a.e.b.c.d / a.e.b.d.c / a.e.c.b.d / a.e.c.d.b / a.e.d.b.c / a.e.d.c.b — 6
b.e.a.c.d / b.e.a.d.c / b.e.c.a.d / b.e.c.d.a / b.e.d.a.c / b.e.d.c.a — 6
c.e. &c — 6
d.e. &c — 6
24

a.b.e.c.d / a.b.e.d.c / a.c.e.b.d / a.c.e.d.b / a.d.e.b.c / a.d.e.c.b — 6
b.a.e.c.d &c — 6
c.a.e.b.d. — 6
d.a.e.b.c. — 6
24

a.b.c.e.d — 24

2. letters can form only 2. series, to wit a.b. and b.a.
add a 3d letter. then it may be inserted in each of these 2 ~~arrangements~~ series either as the 1st, 2d, or 3d letter. consequently there will be 2×3. series = 6 or 1×2×3.
add a 4th letter. as we have seen that 3. letters will make 6. different series, then [the 4th] may be inserted in each of these 6. series either as the 1st. 2d. 3d. or 4th. letter of [the series]. consequently there will be 6×4 series = 24. or 1×2×3×4.
add a 5th letter. as 4. give 24 series, the 5th may be inserted in each of these as the [1st. 2d.] 3d. 4th. or 5th letter of the series. consequently there will be 24×5. series = 120 = 1[×2×3×4×5.]
add a 6th. letter. as 5 give 120 series, the 6th may be inserted in each of these as the 1st. 2d. 3d. 4th. 5[th or 6th] letter of the series. consequently there will be 120×6 series = 720 = 1×2×3×4×5×6.
and so on to any number.
suppose the cylinder be 6 I. long (which probably will be a convenient length, as it [may] be spanned in the hand between the middle finger & thumb of the left hand while in use) [it will] contain 36. wheels, and the num. of it's combinations will be 1×2×3×4×5×6×7×8×9×[10×11]×12×13×14×15×16×17×18×19×20×21×22×23×24×25×26×27×28×29×30×31×32×33×34×35

The wheel cypher.

turn a cylinder of white wood of about 2. I. diam. and 6. or 8. I. long. bore through it's center a hole sufficient to recieve an iron spindle or axis of ⅛ or ¼ I. diam. divide the periphery into 26. equal parts (for the 26. letters of the alphabet) and with a sharp point draw parallel lines through all the points of division from one end to the other of the cylinder, and trace those lines with ink to make them plain. then cut the cylinder crosswise into pieces of about ⅙ of an inch thick. they will resemble backgammon men with plane sides. number each of them as they are cut off on one side, that they may be arrangeable in any order you please. on the periphery of each, & between the black lines, put all the letters of the alphabet, not in their established order, but jumbled & without order so that no two shall be alike. now string them in their numerical order on an iron axis, one end of which has a head, and the other a nut & screw, the use of which is to hold them firm in any given position when you chuse it. they are now ready for use, your correspondent having a similar cylinder similarly arranged.

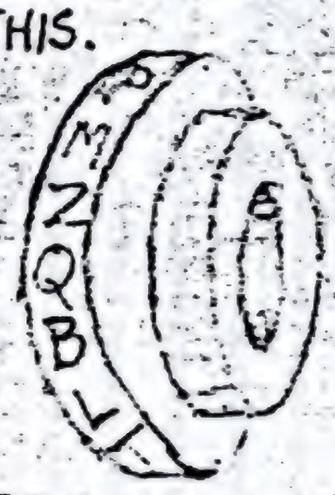
Suppose I have to cypher this phrase 'your favor of the 22d. is recieved'

I turn the 1st. wheel till the letter y presents itself
turn the 2d. and place it's o. by the side of the y. of the 1st.
turn the 3d. and place it's u. by the side of the o. of the 2d.
turn the 4th. and place it's r. by the side of the u. of the 3d.
turn the 5th. and place it's f. by the side of the r. of the 4th.
turn the 6th. and place it's a. by the side of the f. of the 5th.

and so on till I have got all the words of the phrase arranged in one line. you will see that the cylinder then presents 25. other lines of letters, not in any regular series, but jumbled & without order or meaning. copy any one of them in the letter to your correspondent. when he recieves it, he takes his cylinder and arranges the wheels so as to present the same jumbled letters in the same order in one line. he then fixes them with the screw, examines the other 25. lines and finds one of them presenting him these words 'your favor of the 22d. is recieved.' which he writes down. as the others will be jumbled & have no meaning, he cannot mistake the true one intended. so proceed with every other portion of your letter. numbers had better be represented by letters with dots over them, as for instance by the 6. vowels & 4. liquids, because if the periphery were divided into 36. instead of 26. lines for the numerical as well as alphabetical characters, it would increase the trouble of finding the letters on the wheels.

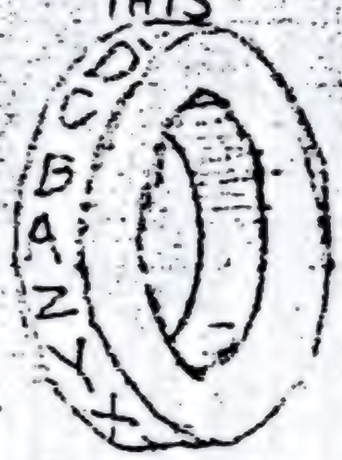
the cypher may be varied for any number of correspondents by varying the arrangement of the wheels. every two of those who possess a set of them may have an arrangement private to themselves, and which cannot be understood by the others.

TEN LIKE THIS.



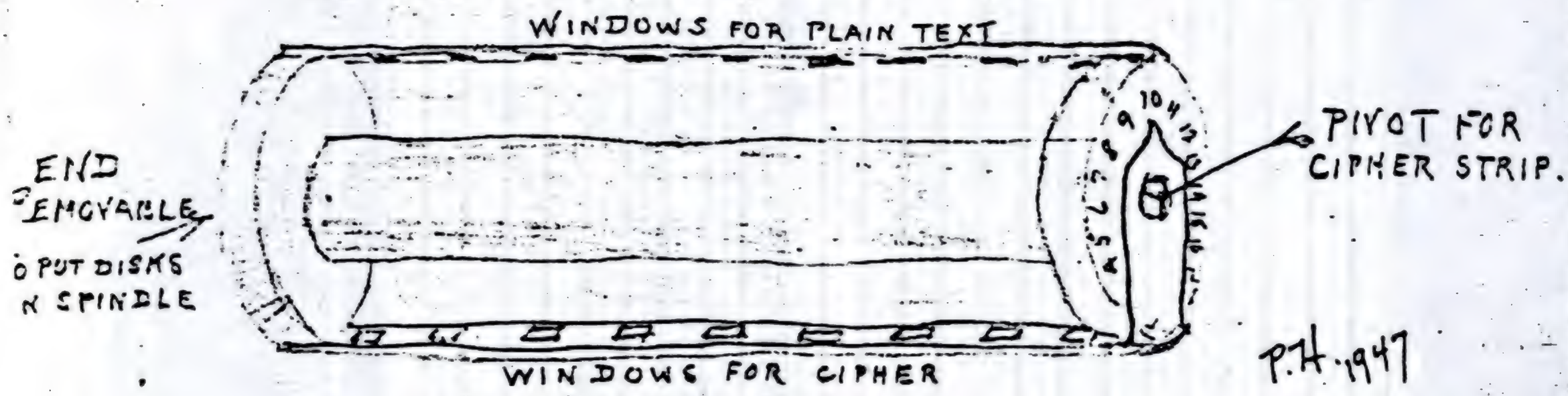
TEN MIXED ALPHABETS

TEN LIKE THIS

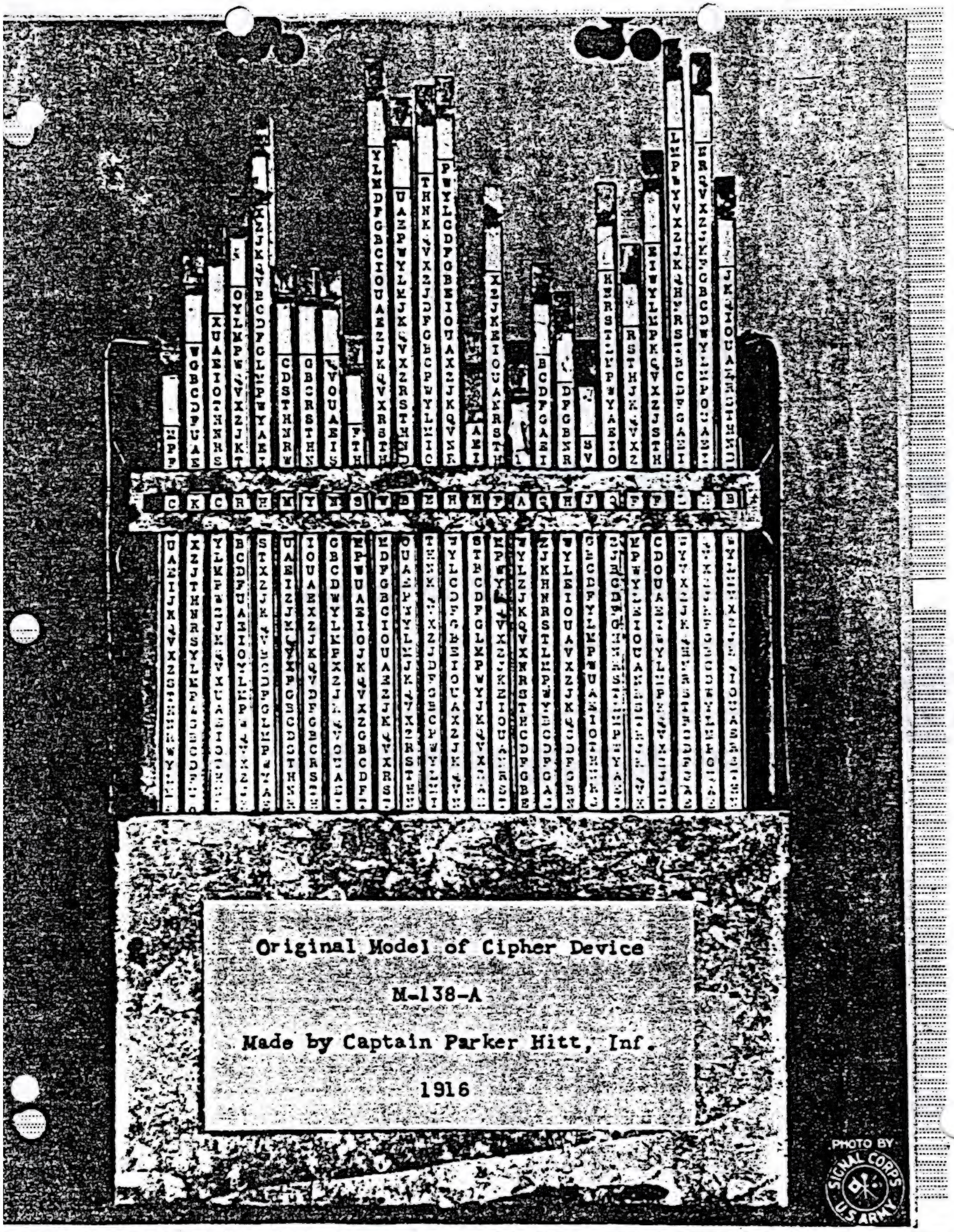


REGULAR ALPHABETS

MY ORIGINAL IDEA (1913) FOR A CIPHER DEVICE.



P.H. 1947



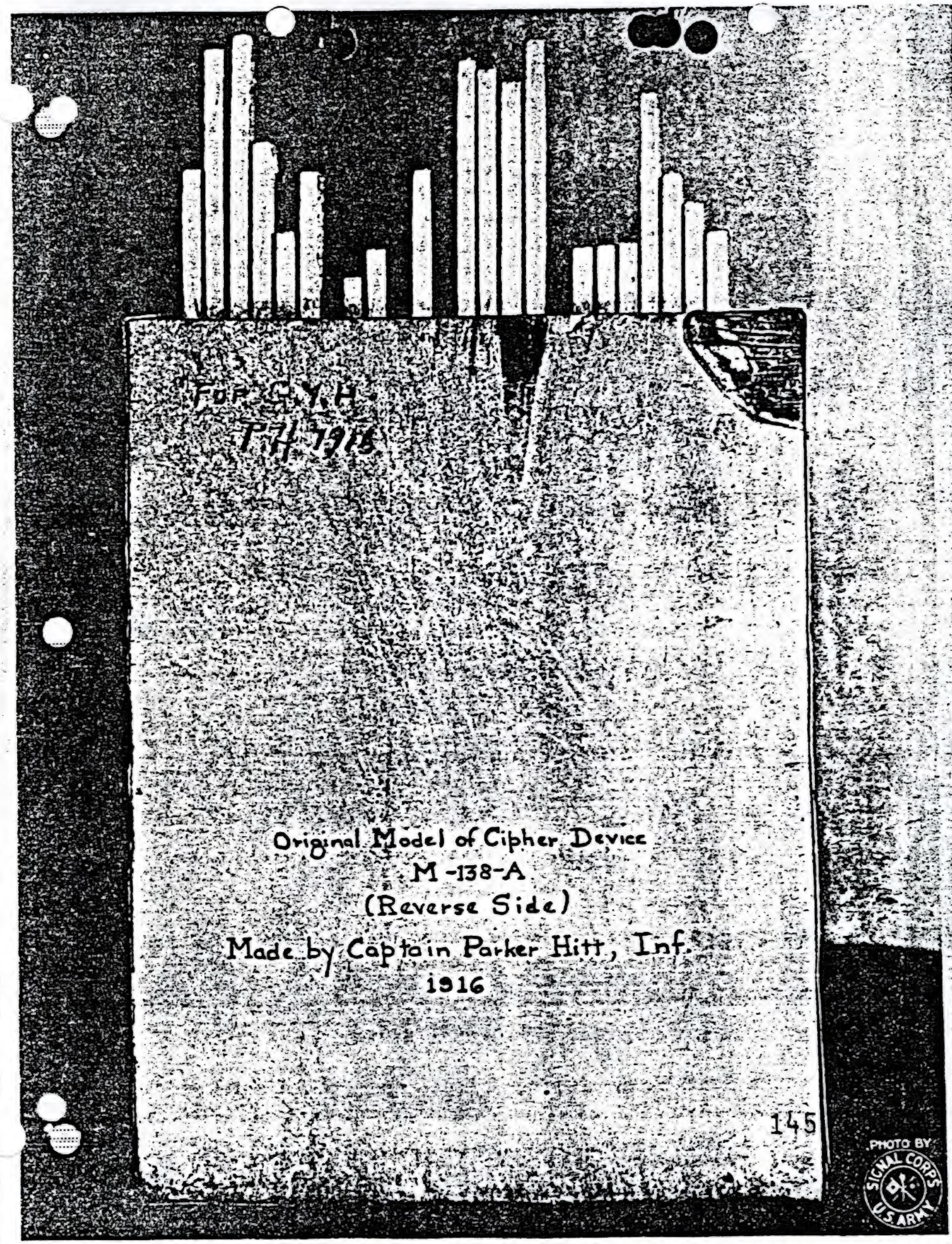
Original Model of Cipher Device

M-138-A

Made by Captain Parker Hitt, Inf.

1916

PHOTO BY SIGNAL CORPS U.S. ARMY



Original Model of Cipher Device
M-138-A
(Reverse Side)
Made by Captain Parker Hitt, Inf.
1916

145

PHOTO BY SIGNAL CORPS U.S. ARMY

Photo No 4

Tab 5, p. 1 of Hist of Strip Cipher Device

This is original pt. of series of 25 msgs Mauborgne submitted as test of Cyl. Cipher Dev

Chlorine and oxygen have not b

VFDJLQMMJBHSYVJKCJTJWDKNI

Where did you meet each other I

CGNJMZVKQCJPRJRCGOXGUCZVC

Drink this potion quickly for

CSTDTSSDJNJDKKTIXVEXVHDVK

Well make me the same shape but

OZBGFVTUECUGTZDKYWJRVZSDG

Cyanogen is a colorless gas in

CIRMBFTKBYCGAQVDQCVQAHZGY

Phenols are benzene derivati

VQWRMIHDHBRQBWULKJCSKEYUU

Xylonite and artificial ivor

SSEIQDWHNHQHGIKHAADNGNFBY

I went to a new theatre the Pala

VXDVXNIGJOPCOTNGKWAXYTNWL

Picric acid is explosive and I

QJRLHAWTWUCYXVMBGJCRSBHWF

Llangollen is a town in Wales a

DULPKUXMVLXFUPSULRZKPDALY

"vette are you going shopping

DCAIYLUPMBNACQEOPTLHKKRGT

Orthophosphoric is the compo

VIGODTVGUYXNHKBEWPOVRVTQOE

Caoutchouc is closely allied

TBVEBQDXGPLCPUYAVYBKZEOZY

Olefiant gas ethene or ethyle

FIJDWWBKTYGBSMBPZWYPRRZCW

See the terrible tank tackle a

DYVPJCLNXESCMFOYPIZFPEBHM

It is a thin limpid liquid that

YYTJRFMEPPHDXPODFZOWLGLA

It it is insoluble in water it i

EYKKDXHTEVTRXWKCJPSGMASCY

Silver has been known from rem

LGQLVHTUIPYAUGJPGDLHVZTKV

Hot concentrated sulphuric a

BRKTJRGGTBHMLXXFRHOAAZVWU

Small coefficient of expansi

CDUDVDBZUAELRPOSPUJDXRZWA

Palladium possess a power o

EUFBTTWNIYHHTNWQNFVENYGBY

Cleaning and cansing thi

TUTVYNGLPGTYOLIHXZQTXSGOJ

Compounds of platinum form for

PBTJC CJONJ UNIXB UAQBI WNIHL

Gold occurs widely distribut

VHNKR XVZMD KFHUY XRNDD KXXYM

Oxidation caused by it probab

NNHBF VQHOB LXCYM AKFLS SSJXG

VFDJL QMMJB HSIVJ KCJTJ MDKMI

CGMJM ZVKQC JPRJR CGOXG UCZVC

CSIDI SSDJM JDKKI IXVKX VHDJK

OZBGI VIUKC UGIZD KYMJR VZSDG

QIRMB FIKBI GGAQV DQGVQ AHZGI

VQMRM IHDHB RQBMU LKJGB KEYUU

SSEIQ DWHMH QHGIK HADDM GMFBY

VXDVX MIGJO PCOIM GKMAX YIMWL

QJRLH AMIWU CYXVM BGJGR SBHWF

DULPK UXMVL XFUPS ULRZK PDALY

DCAIY LUPMB MACQM OPILH KKRGT

MGODI VGUYX HHKBE MPOUR VTQOM

IBVKB QDXGP LCPUY AVVBK ZEOZY

FIJDM WBKTY GBSMB PZMYP RRZGW

DYVPJ CLMXK SGHFO YPIZF PKBHM

MYYIJ RFMBP PHDIP ODFZO WLGLA

KYKKD XHIEV IRXMK CJPBG MASGY

LGQLV HTUIP YAUGJ PGDLH UZIKV

BRKIJ RGGIB HMLXX FRHOA AZVMU

CDUDV DBZUA ELRPO SPUJD XRZWA

KUFBI IWHIY HHIMW QHFVE MYGBY

IUIVY MGLPG IYOLI HXZQI XSGOJ

PBIJC CJOHJ UNIXB UAQBI WHIHL

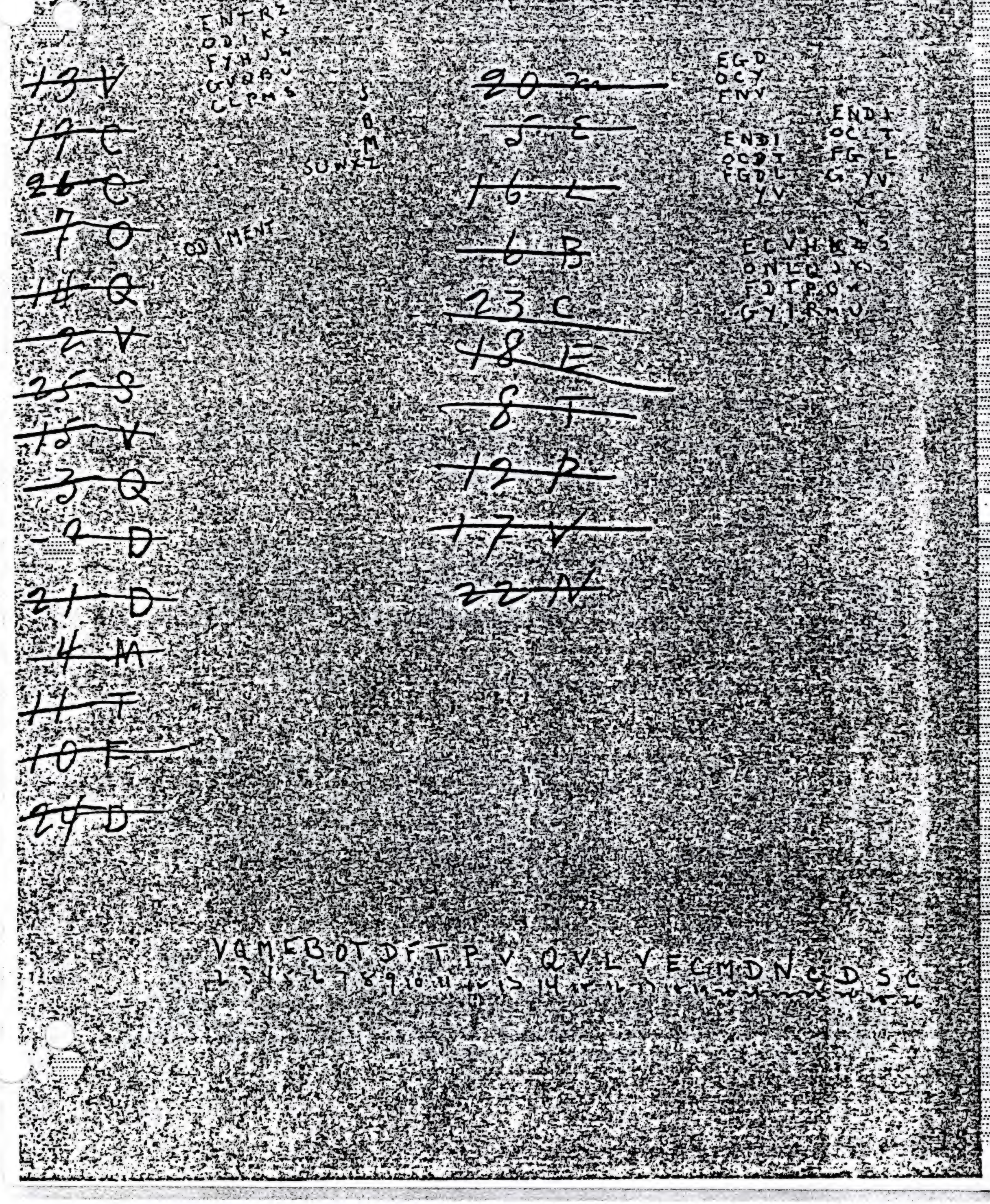
VHMKR XVZMD XFHUY XRMDD KXXVM

MMHBF VQ HOB LXGYM AKFLS SSJXG

Copy furnished to Cipher Bureau
Apr. 23, 1918.

Set up of disks

E9FGCNDYVLTIHQPRKJBMZXWUS



Signal Corps,
U. S. Army Specification.

No. 72-26
May 20, 1921.

CIPHER DEVICE, Type M-94.

* * * * * * * *

1. General.

This specification describes a device consisting of a number of discs with parts for assembling, to be used in enciphering and deciphering messages transmitted by telegraphic code. The periphery of each disc shall be marked with every letter of the alphabet and when assembled the discs may be turned in either direction permitting any letter to be brought to the desired position. When the required combination of letters is formed, the discs can be secured to retain that combination.

2. Material and Workmanship.

All parts, except where otherwise specified, shall be made of an aluminum alloy of the best quality for the purpose. The workmanship shall be of the highest grade throughout.

3. Drawing.

The following drawing forms a part of this specification. Details shown on the drawing and not referred to in the specification, and vice versa, should be considered as in both. Revised drawings are indicated by a suffix number. Each succeeding revision is indicated by a higher order of number.

(a) Cipher Device, Type M-94, ... 50306B1.

4. Description.

All parts shall be of dimensions shown on drawing, section 3(a). The discs shall be die castings of best quality, free from rough edges and defects. One side of the disc shall be provided with twenty-six (26) gear teeth equally spaced and the stud for meshing with the gear of adjoining discs shall be located opposite a point midway between the letter A and the letter above it. The rod and thumb nut shall be accurately machined and threaded.

5. Lettering.

The periphery of each disc shall be stamped with every letter of the alphabet, equally spaced, the height and style of letters to be as shown on drawing, section 3(a). The discs shall be serially numbered from one (1) to twenty-five (25) inclusive and also lettered consecutively from "3" to "Z", the marking to be located as shown on drawing, section

section 3(a). All letters and figures shall be stamped into the metal and filled with black enamel of best quality that will not chip or peal.

The lettering on the periphery of the discs shall be arranged in accordance with the following table. The letters in the first column on the left shall be shown on disc marked 1 - B and each disk of a higher order of number shall be marked with letters in the succeeding columns in the order given.

A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	D	K	D	M	P	X	H	D	E	T	N	C	D	B	J	M	D	O	T	N	V	K	J	D
E	E	O	C	Q	O	J	P	S	L	M	F	J	W	V	N	Y	M	J	R	K	S	W	P	N
I	H	M	B	U	C	E	J	X	B	S	L	I	P	H	U	O	C	Y	Z	H	F	R	X	B
G	F	J	I	K	I	Z	O	Q	D	X	H	L	K	I	B	F	N	L	X	R	D	E	M	U
D	I	U	F	D	X	B	B	O	F	V	Q	D	J	Y	T	T	E	F	Q	G	L	V	V	H
J	J	B	G	O	L	N	W	I	J	Q	G	H	V	K	G	H	Q	X	L	O	I	D	K	Y
F	K	G	J	P	U	I	K	V	G	P	C	B	I	S	I	E	B	N	Y	X	E	T	B	F
V	T	E	H	I	R	K	C	T	H	N	U	M	U	G	M	U	O	G	I	E	B	U	Q	W
U	L	P	L	T	N	P	V	Z	O	O	J	K	Q	U	W	S	Z	M	O	Y	H	F	W	J
Y	M	H	K	J	D	V	F	E	N	H	T	G	H	E	Z	Z	P	H	V	B	K	O	U	L
M	O	S	M	B	Y	R	Z	F	M	U	B	X	Z	N	R	J	L	V	B	F	N	Y	G	V
H	U	C	R	R	Z	O	L	H	T	W	Y	U	C	T	V	X	G	C	P	S	R	H	L	G
T	V	Z	U	H	H	G	Q	G	P	D	P	Z	T	C	L	D	V	M	E	J	W	M	O	R
Q	Y	I	O	C	W	S	E	Y	R	I	Z	T	X	X	X	P	J	I	S	M	Q	L	S	C
K	G	N	Q	Y	B	Y	R	U	Q	Z	K	S	B	O	C	C	R	R	N	U	Z	S	T	Q
Z	Z	X	V	S	J	D	Y	N	S	Y	X	W	L	W	S	W	K	B	H	D	G	I	E	M
O	N	F	P	L	S	U	N	L	V	C	I	Q	E	F	H	G	Y	S	J	Q	M	Q	C	P
L	P	Y	T	W	Q	L	S	P	Z	G	S	Y	G	Q	D	Q	T	E	W	C	X	N	H	S
R	Q	Q	N	E	F	C	U	M	U	K	R	V	N	D	E	I	F	K	M	L	P	J	N	O
X	X	R	W	M	K	F	M	B	X	R	D	O	Y	R	O	B	U	U	D	Z	U	C	Z	E
S	R	T	Y	Z	V	M	G	X	Y	F	V	R	R	L	K	K	I	P	G	W	C	P	F	X
P	W	V	X	V	H	Q	T	W	W	B	E	P	S	J	F	L	W	D	F	T	O	G	R	T
W	S	W	Z	X	E	T	D	C	I	E	W	F	M	Z	P	N	X	Z	C	I	T	B	I	K
N	B	L	S	G	T	W	X	R	C	J	O	E	F	M	Y	V	H	Q	K	P	Y	Z	D	I

6. Requirements.

The dimensions shown on drawing, section 3(a), shall be followed closely, the usual variation allowable in shop practice being permitted. The variation in di mensions of the spaces between gear teeth and the thickness of the stud which meshes with the gears, shall be such that when the discs are assembled with their adjoining sides in contact, there will be only sufficient rotary movement to permit a fixed point on the circumference of an end disk to pass over an arc not more than seven-thirty-seconds (7-32) of an inch long when the disc at the opposite end of the cipher device is stationary.

7. Identification Code Marking.

The disc, detail #2, drawing, section 3(a) shall be stamped as

follows:

Cipher Device
Type M-94
Signal Corps
U. S. Army.

The letters shall be arranged as shown on the drawing and filled with black enamel.

8. Inspection.

All material, unless otherwise specified, shall be inspected before shipment is made, and the contractor shall notify the inspecting officer named in the order in sufficient time to avoid any delay in the shipment.

9. Packing and Marking.

The cipher device shall be wrapped in tissue paper and placed in paper boxes containing six units, then packed in the usual commercial manner to withstand shipment to any part of the United States. If extra or special packing is required for any unusual or foreign shipment, the contractor will be made the proper allowance to cover this work. The contractor will be held responsible for any damage in transit or handling resulting from faulty packing.

The boxes shall be properly stenciled, showing the Signal Corps order number, and the name and number of articles therein, in addition to the destination and other shipping instructions.

Unless otherwise specified, government bill of lading will be furnished covering the shipment.

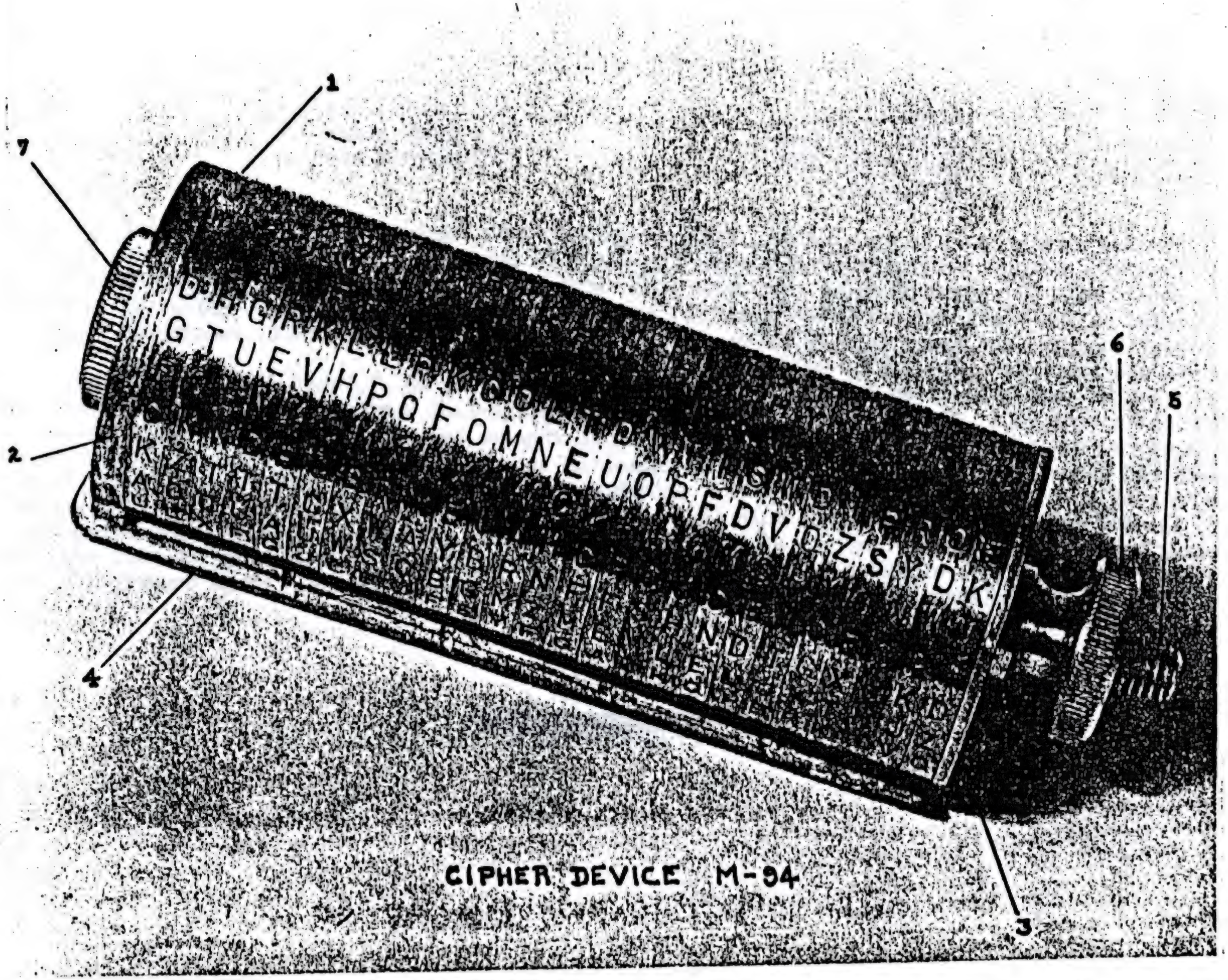
DETAILED DESCRIPTION OF CIPHER DEVICE M-94

Photograph Opposite

1 - Alphabet disk
2 - Guide rule disk
3 - Name plate disk
4 - Guide rule
5 - Central shaft
6 - Thumb screw
7 - Knurled knob

Cipher Device M-94 is an aluminum device composed of 27 removable disks (diameter: 1 7/8 in.) mounted on a slender central shaft (length: 4½ in.). At the left end of the central shaft (5) is a knurled knob (7) which prevents the disks from sliding off. One inch of the central shaft (5) is threaded at the right end. A thumb screw (6) on this threaded end of the shaft holds the 27 disks tightly together and keeps them in place. To remove the disks from the shaft, remove the thumb screw and the disks will easily slide off.

The 27 removable disks consist of the guide-rule disk (2), 25 alphabet disk (1), and one nameplate disk (3). The guide-rule disk contains one plain flat surface and a cupped surface. On the cupped surface is a tiny raised projection which engages one of the notches on the adjacent disk and locks (Tab B). A hole through the center of the disk is just large enough to allow it to slip easily on and off the central shaft. Attached to the blank rim of the guide-rule disk is a 3½ in. extension, called the guide rule (4). The guide-rule can be rotated on the shaft so as to bring the guide rule under any one of the 26 horizontal lines of letters formed by the alignment of the letters of the alphabet disks. The guide rule contains four notches along the top edge for the purpose of dividing a horizontal line of letters into 5-letter groups. (This description is continued in Tab 8.)



CIPHER DEVICE M-94

DETAILED DESCRIPTION OF CIPHER DEVICE M-94 (Cont.)

Photograph Opposite

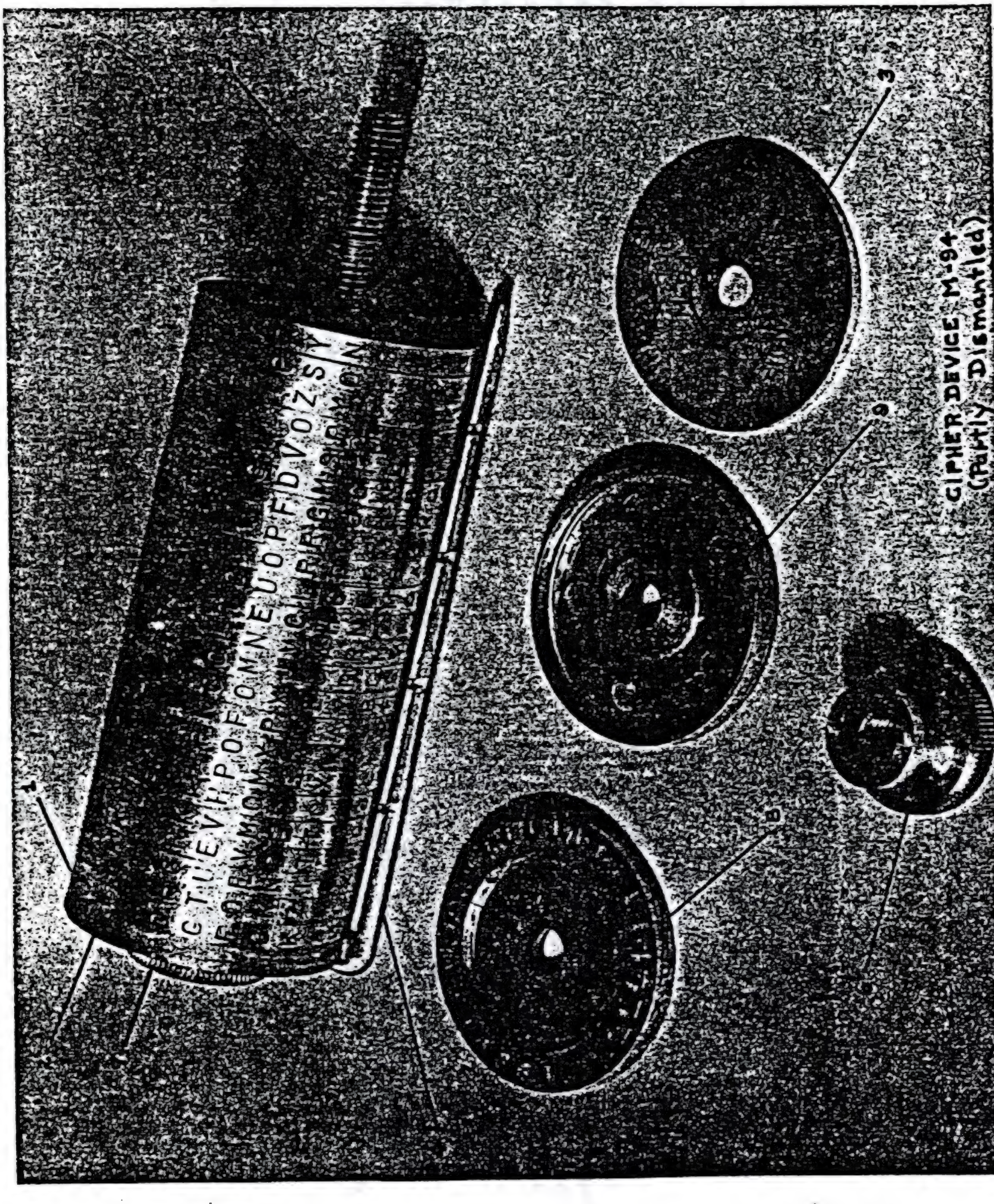
1 - Alphabet disk
2 - Guide rule disk
3 - Nameplate disk
4 - Guide rule
5 - Central shaft
6 - Thumb screw
7 - Knurled knob
8 - Plain flat surface of alphabet disk
9 - Cupped surface of alphabet disk

The 25 alphabet disks each have upon their rim a completely random alphabet. On one side of each alphabet disk are 26 notches (8); one of these notches engages the tiny raised projection on the cupped surface (9) of the disk just to the left. When the disks are locked in this manner, they are so positioned that 26 horizontal lines of letters appear on the outside of the device. Besides the tiny raised projection, the cupped surface (9) of each alphabet disk contains a letter and a number. The disks are numbered from 1-25 and lettered from B-Z.

To prepare the device for encipherment, the disks must be placed on the shaft in a prearranged order. The means actually used for determining this order was a numerical sequence of 23 numbers derived from a key word or key phrase.[1] After the alphabet disks have been placed on the shaft in accordance with the prearranged numerical sequence, the device is ready for aligning the first 25 letters of plain text. By revolving the alphabet disks upon the shaft one by one, the first 25 letters of the message must be brought all upon the same horizontal line. As a letter on each new disk is aligned, the disk may be locked with the one adjacent at its left. The guide rule may be placed under the line of letters being aligned. When all 25 letters have been aligned, the cipher-text line is chosen at random from any one of the other 25 horizontal lines. To aid in copying the cipher text, the guide-rule disk may be disengaged and placed underneath the cipher-text. The cipher text is copied in groups of 5 letters. The notches on the guide rule will indicate the division of the line of letters into groups of five. All successive lines of 25 letters are enciphered in the same manner. Decipherment is performed by aligning one line of cipher text at a time and finding the only readable line (the plain text) among the other 25 horizontal lines of letters.

---

1. The derivation of a numerical sequence is explained on a page following this photograph.



CIPHER DEVICE M-94
(Partly Dismantled)

DERIVATION OF A NUMERICAL SEQUENCE

To derive a numerical sequence from a key word or key phrase, proceed as follows: Write a series of numbers (in this case, 1-25 because there are 25 alphabet disks) and write the letters of the key word or key phrase beneath the numbers, repeating the beginning of the phrase if necessary. An example, using the key phrase, UNITED STATES OF AMERICA, is shown below:

1 -2 -3 -4 -5 -6 -7 -8 -9 -10-11-12-13-14-15-16-17-18-19-20-21-22-23-24-25
U N I T E D S T A T E S O F A M E R I C A U N I T

Now proceed to place numbers under the letters in accordance with their relative positions in the ordinary alphabet, that is, "A", if present, is given the number 1 and further occurrences of "A", if present, are given the numbers 2, 3, etc., "B", if present, is given the next number, and so on, working from left to right, until every letter has been assigned a number. If the work is correctly completed, every letter will have a number beneath it and the greatest number will be the last number in the series written above it. If the letter "A" does not appear in the key word or phrase, then the first letter of the alphabet that does appear is given the number 1. The same is true as the work proceeds. When the next letter of the alphabet does not appear in the key, assign the next greatest number to the next letter of the alphabet which does appear in the key. Continuing the example, the final result will be as follows:

1 -2 -3 -4 -5 -6 -7 -8 -9 -10-11-12-13-14-15-16-17-18-19-20-21-22-23-24-25
U N I T E D S T A T E S O F A M E R I C A U N I T
24-14-10-20-6 -5 -18-21-1 -22-7 -19-16-9 -2 -13-8 -17-11-4 -3 -25-15-12-23

~~SECRET~~

DETAILED DESCRIPTION OF CIPHER DEVICE M-136

Photograph Opposite

1 - Central Shaft
2 - Metal base
3 - Bench-mark disk
4 - Alphabet disk
5 - Thumb screw disk
6 - Removable rod
7 - Bakelite plug

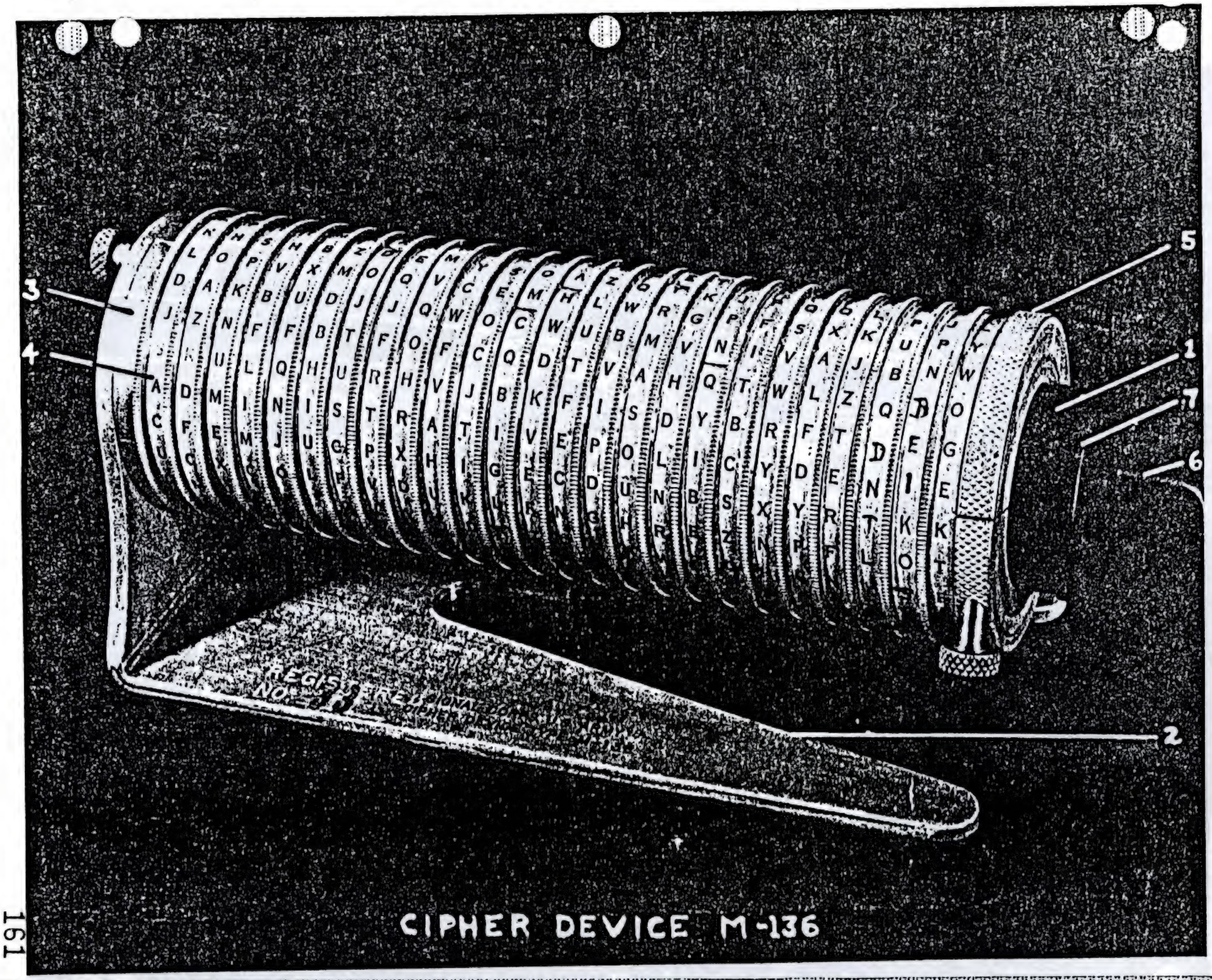
The numbers 1, 2, etc. listed here and appearing parenthetically within the text below, refer to the numbers in the photographs.

Cipher Device M-136, which is approximately 9 inches long, consists of 27 aluminum disk (diameter: 2 7/8 in.) mounted on a large hollow central shaft (diameter: 1 3/4 in.) of bakelite. The central shaft (1) is attached to a metal side piece at the left end. The device is supported by a metal base (2) made by a curve and an extension of the left side piece. The 27 disks, one "bench-mark" disk (3), 25 alphabet disk (4) and one thumb-screw disk (5), are located on the central shaft from left to right in the order named. When mounted, the disks are held in place by the thumb screw at the top of the left side piece, the thumb screw on the thumb screw disk, and the long thin removable rod (6) which is curved on one end. When the device is assembled, the curved end of the rod protrudes from the right end. At the right end of the hollow bakelite shaft is a bakelite plug (7) which is removable; this feature allows the bakelite shaft to be used as a container.

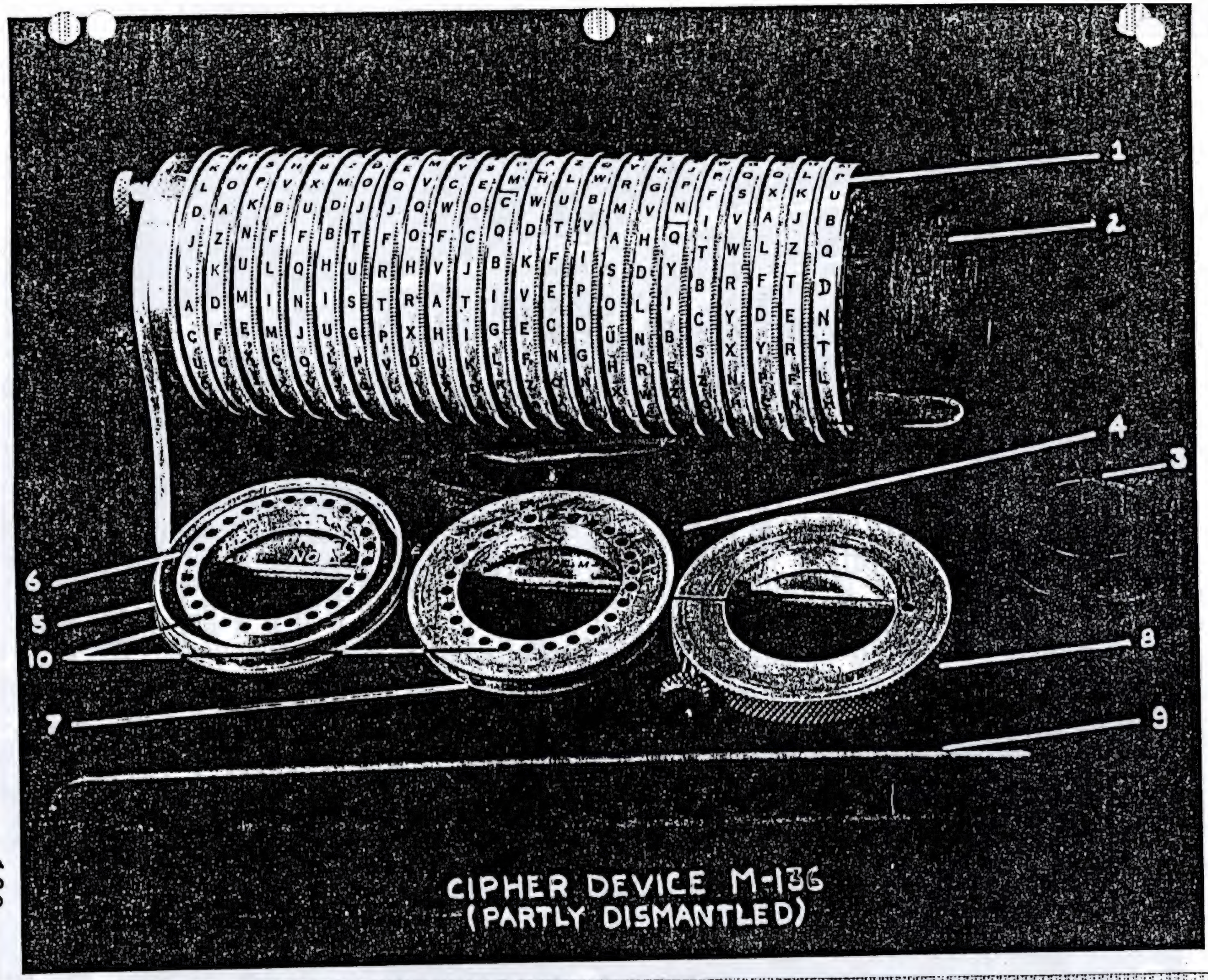
To remove the disks from the device, the removable rod must be pulled out and the bakelite plug removed. The thumb screw in the thumb screw disk on the extreme right must be loosened. The loosening of this screw makes the central hole of the thumb screw disk (5) larger and allows the disk to slip off the shaft. All other disks are constructed to slip off without adjustment.

The "bench-mark" disk (3) is located at the extreme left between the left side piece and the first alphabet disk. The 26 "bench-marks" appearing on its periphery aid in alignment of the letters on the alphabet disks. (This description is continued in Tab 10.)

~~SECRET~~



CIPHER DEVICE M-136



CIPHER DEVICE M-136
(PARTLY DISMANTLED)

~~SECRET~~

DETAILED DESCRIPTION OF CIPHER DEVICE K-136 (Con't.)

Photograph Opposite

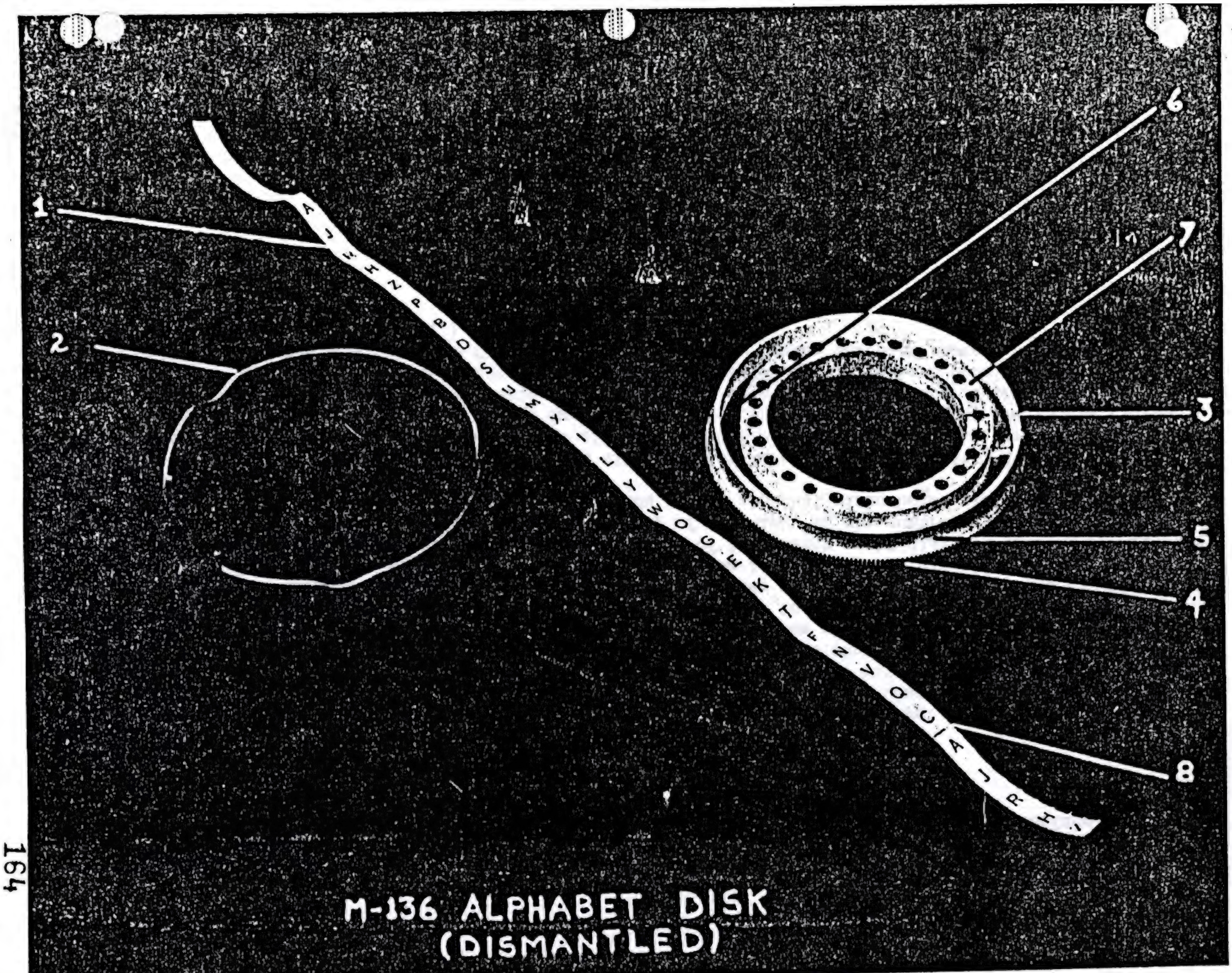
1 - Alphabet disk (cupped surface exposed)
2 - Central shaft (with three disks removed)
3 - Bakelite plug
4 - Metal base
5 - Alphabet disk (cupped surface upward)
6 - Wire spring
7 - Alphabet disk (flat surface upward)
8 - Thumb screw disk
9 - Removable rod
10 - Small holes

Each alphabet disk contains 26 small holes (10) through its flat sides. These small holes are evenly spaced and form a border around the large middle hole. On the bench mark disk these small holes have two uses: the thumb screw at the top center of the left side piece fits into one of these 26 holes and helps to hold the disks in place when aligned; The straight end of the curved rod also fits into one of these holes, after having been run through the other 26 disks.

The alphabet disks (1) all 25 of which are located just to the left of the "bench mark" disk, have a paper alphabet strip mounted on the rims. The disks each have a cupped surface (5) and a flat surface (7). They are numbered on their flat sides from 1-25. With the exception of the number, the flat side of an alphabet disk and the flat side of the "bench mark" disk are exactly alike. The numbers are for the purpose of changing the order of the disks on the central shaft according to a prearranged numerical sequence. The cupped side of the alphabet disks holds small metal wires (6) which keep the paper strips in place

The rim of an alphabet disk, as viewed with the disk in a vertical position, is composed of a thin ridged edge, and a wider smooth edge slightly below the ridged edge. Paper strips containing scrambled alphabet are mounted on the smooth edge. When the disks are mounted, the raised ridged edge keeps the paper strips from slipping from side to side. Removable paper alphabet strips are used to permit substitution of completely new sets of strips. This feature provides the security improvement over Cipher Device K-94 for which purpose the device was constructed. (This description is continued in Tab 11.)

~~SECRET~~



M-136 ALPHABET DISK
(DISMANTLED)

DETAILED DESCRIPTION OF CIPHER DEVICE C-136 (Cont.)

Photograph Opposite

1 - Alphabet strip
2 - Wire spring
3 - Slit
4 - Ridged edge
5 - Smooth edge
6 - Hollow
7 - Raised portion containing holes
8 - Black line

Each alphabet strip (1) contains a complete scrambled alphabet. The letters are spaced exactly the same distance apart to permit horizontal alignment of letters when the disks are mounted on the central shaft. Directly above the alphabet is a black line which divides the alphabet from the number on the strip. (The strips are numbered from 1-25.) Above the number is about 2 3/4 inches of blank strip. Below the alphabet is a black line (8) which divides the alphabet from the beginning of a repetition of it. The repetition is torn off about 2 3/4 inches below the black line so that only five or six letters of the repetition appear on the strip. The space (in which one complete random alphabet is printed) between the black lines is 8 3/4 inches as is the circumference of the smooth edge of the alphabet disk on which the strip is mounted. The strip is 1/4 inch wide which is also the width of smooth edge of the alphabet disk.

When a strip is to be mounted on the smooth edge of an alphabet disk, it is first folded on the black lines above and below the complete random alphabet. It is then fitted, at the folds, into the tiny slit (3) in the smooth edge of the disk so that the part of the strip containing the random alphabet will fit around the outside of the disk (5). The ends of the strip which fit through the tiny slit curl around into the little hollow (6) between the narrow smooth edge and the raised portion of the disk containing the border of small holes. The strips are held snugly in place by a wire spring (2) which fits into the little hollow and presses the ends of the strips tightly against the sides. The number of the strip corresponds to the number of the disk on which it is mounted.

When all strips are mounted and the disks placed on the shaft in key-number order, the disks can be locked in place as follows: Place the end of the rod through the hole in the thumb-screw disk, then run it through corresponding holes of all 26 other disks. (So that the holes will be properly positioned for running the rod through them, the letters on the alphabet disks must be positioned so that they form horizontal lines of letters.) Tighten the thumb screw on the security disk. Replace the plug in the mouth of the central shaft.

DETAILED DESCRIPTION OF CIPHER DEVICE K-137

Photograph Opposite

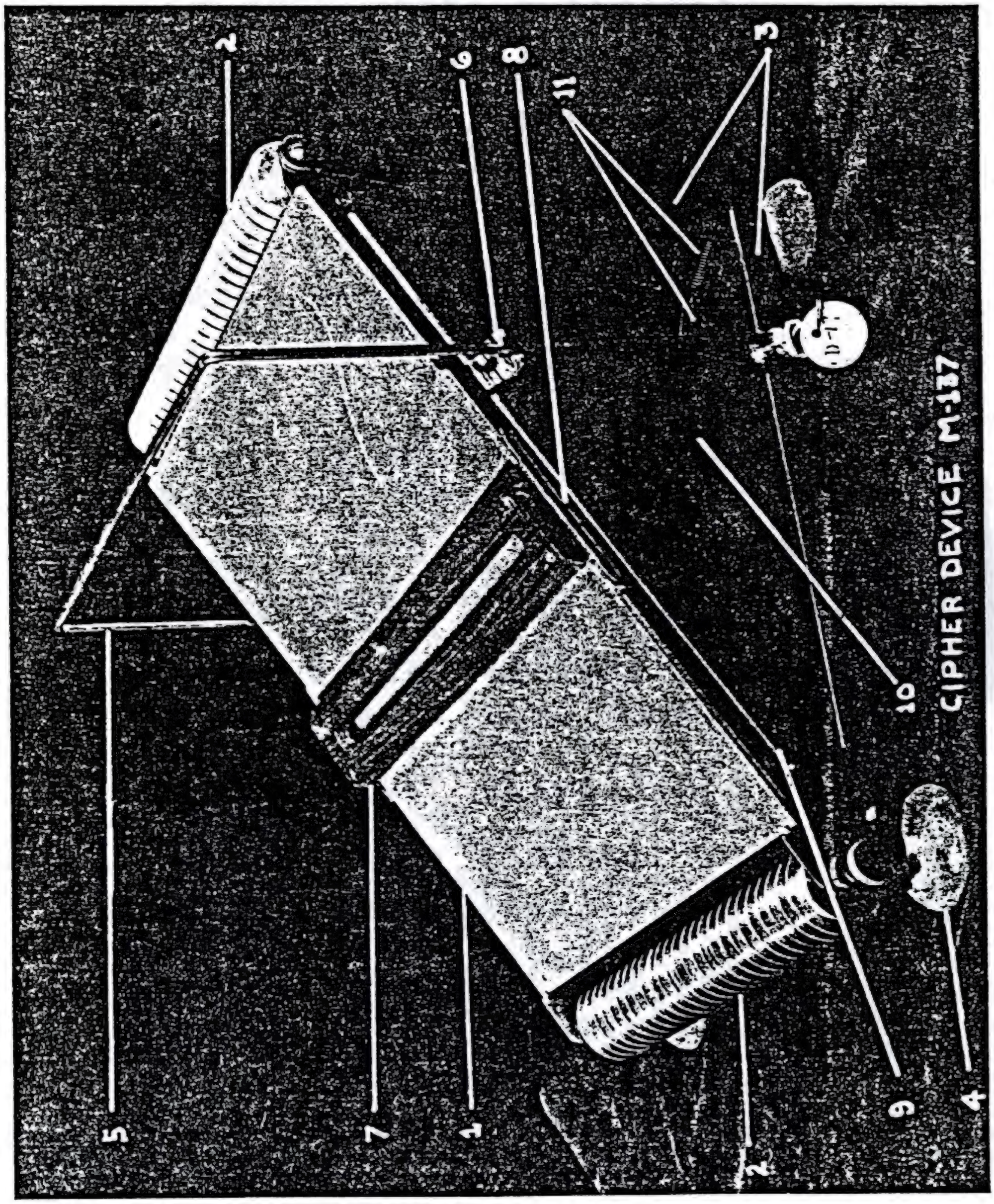
1 - Aluminum plate
2 - Pulley wheels
3 - Aluminum frame
4 - Rubber legs
5 - Lever
6 - Bar
7 - Wooden guide rule
8 - Metal slide
9 - Cylindrical rod
10 - Turning rod
11 - Arm and spring

Cipher Device K-137 consists of an aluminum plate (1) (11" x 10½") above and below which are attached 25 pulley wheels (2). The aluminum plate is supported at a 45° angle by an aluminum frame (3). The device is designed in this manner so that 25 alphabet strips can be stretched across the plate and over the pully wheels; the ends of each strip are clamped together underneath the aluminum plate by means of individual coil springs. The device rests on four small rubber legs (4).

A lever (5) attached to the base of the aluminum frame, and extending above and across the aluminum plate, operates a bar (6) underneath the metal plate. This lever and attached bar perform the function of returning the alphabet strips to their original positions after enciphering each line of letters. A movable wooden guide rule (7) with reading slot extends horizontally across the aluminum plate. It is attached to the edges of the aluminum plate by means of a metal slide (8). The metal slide, held in place on the one side by a spring clip, allows the reading guide to be moved all the way up and down the aluminum plate. To facilitate changing the alphabet strips, the reading guide can be removed from the device by sliding it off the top of the aluminum plate.

No instructions are available on use of Cipher Device K-137. Neither are the alphabet strips available. However, the arrangement of the reading guide for horizontal reading shows that the letters of the mixed alphabets were printed vertically. The method of operation is to align 25 letters of plain text horizontally across the device, probably within the reading guide, by pushing the strips individually. The cipher-text line would then be chosen at random and the reading guide moved to enclose it as an aid to copying.

The coil springs, (unobtainable for photographing) which hold the ends of the alphabet strips together beneath the device, require the complicated lever (5) and bar (6) arrangement. At the start of encipherment, all the coil springs are brought to the lower end of the aluminum plate by pulling the lever down. Description continued in Tab 13.


CIPHER DEVICE M-137

[redacted]

DETAILED DESCRIPTION OF CIPHER DEVICE M-137 (Cont.)

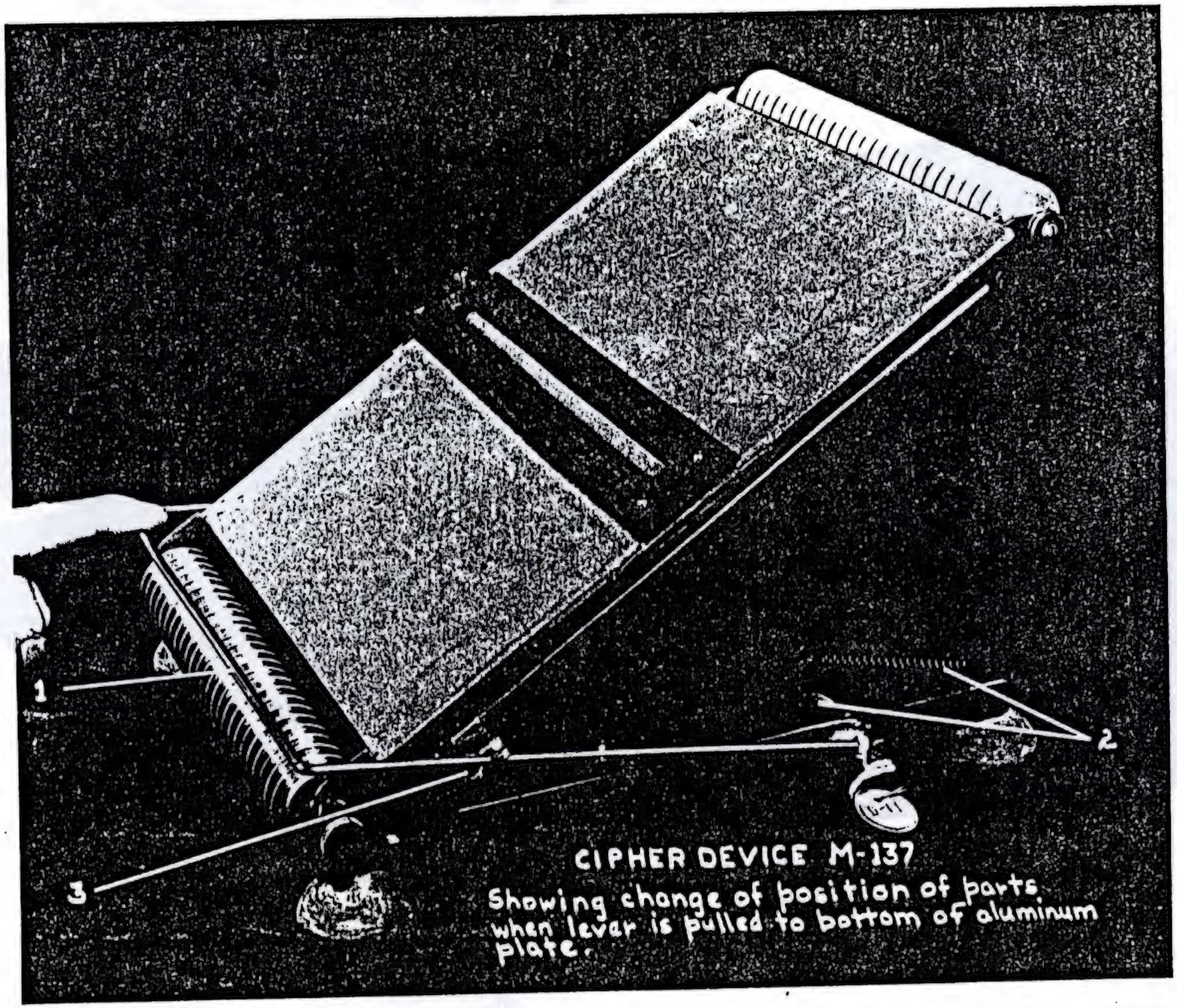
Photograph Opposite

1 - Lever pulled down
2 - Arm and spring
3 - Bar attachment

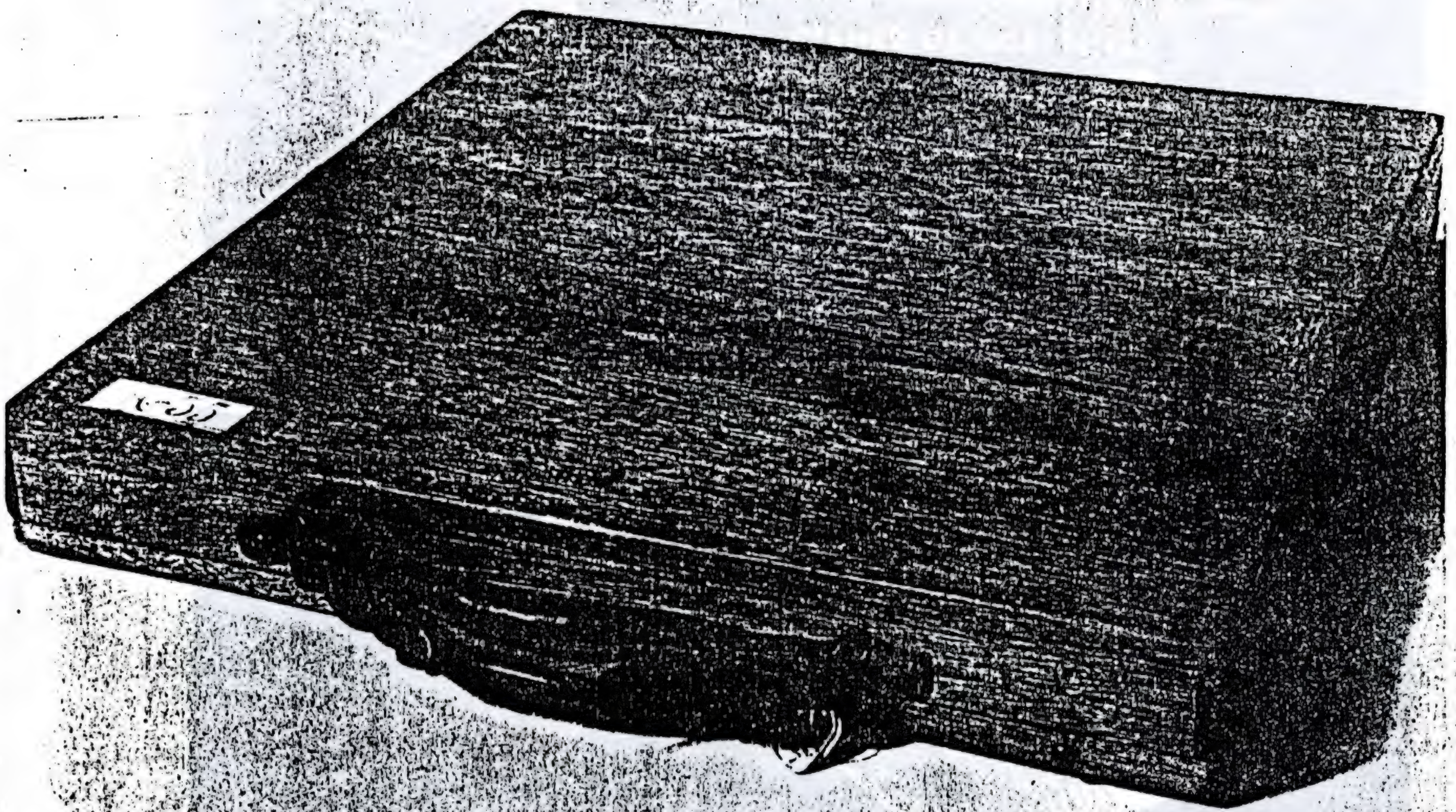
When a strip is moved downward for the purpose of placing a letter within the reading guide, the coil spring holding the ends of that strip together underneath the aluminum plate, automatically moves up. Therefore, when 25 letters of plain text have been aligned across the device, all the coil springs will have moved up in accordance with how much the alphabet strips were moved down. Since neither the alphabet strips nor the coil springs are available for photographing, it is necessary to imagine a line of plain-text letters within the reading guide slot while the coil springs are positioned irregularly underneath the aluminum plate. If another line of plain text aligned without returning the coil springs to the lower end of the aluminum plate, some of the coil springs would become entangled with the bar attachment. Therefore, the coil springs are brought to the bottom of the aluminum plate by pulling the lever down, which action drags the bar attachment (3) downward along the cylindrical rods to which it is attached. The lever moves down by means of the turning rod attached to the base of the metal frame; as the lever comes down, the rod turns toward the front. As the bar attachment slides downward, it engages the coil springs, carrying them to the lower end of the aluminum plate and thus preparing the device for encipherment of the next 25 letters of plain text. This procedure is informally called "zeroizing". This operation also enabled the encipherer to familiarize himself with the position of the letters on the alphabet strips, since it returned the letters of the alphabet to the same position each time the lever was lowered. When the lever is released, the arm and spring (2) attached to the right end of the turning rod, snaps the lever back into its rest position at the top of the aluminum plate.

The 25 pulley wheels above the aluminum plate are mounted on a shaft and the shaft is attached to the metal frame by means of screws. The 25 pulley wheels below the aluminum plate are mounted on a shaft and the shaft attached to the aluminum plate by means of thumb screws which fit into the ends of the shaft through $\frac{1}{2}$ inch slots in the base of the aluminum frame. The thumb screws in the end of the lower pulley-wheel shaft can be loosened and the shaft slid up or down in the slots for the purpose of adjusting the tension of the alphabet strips.

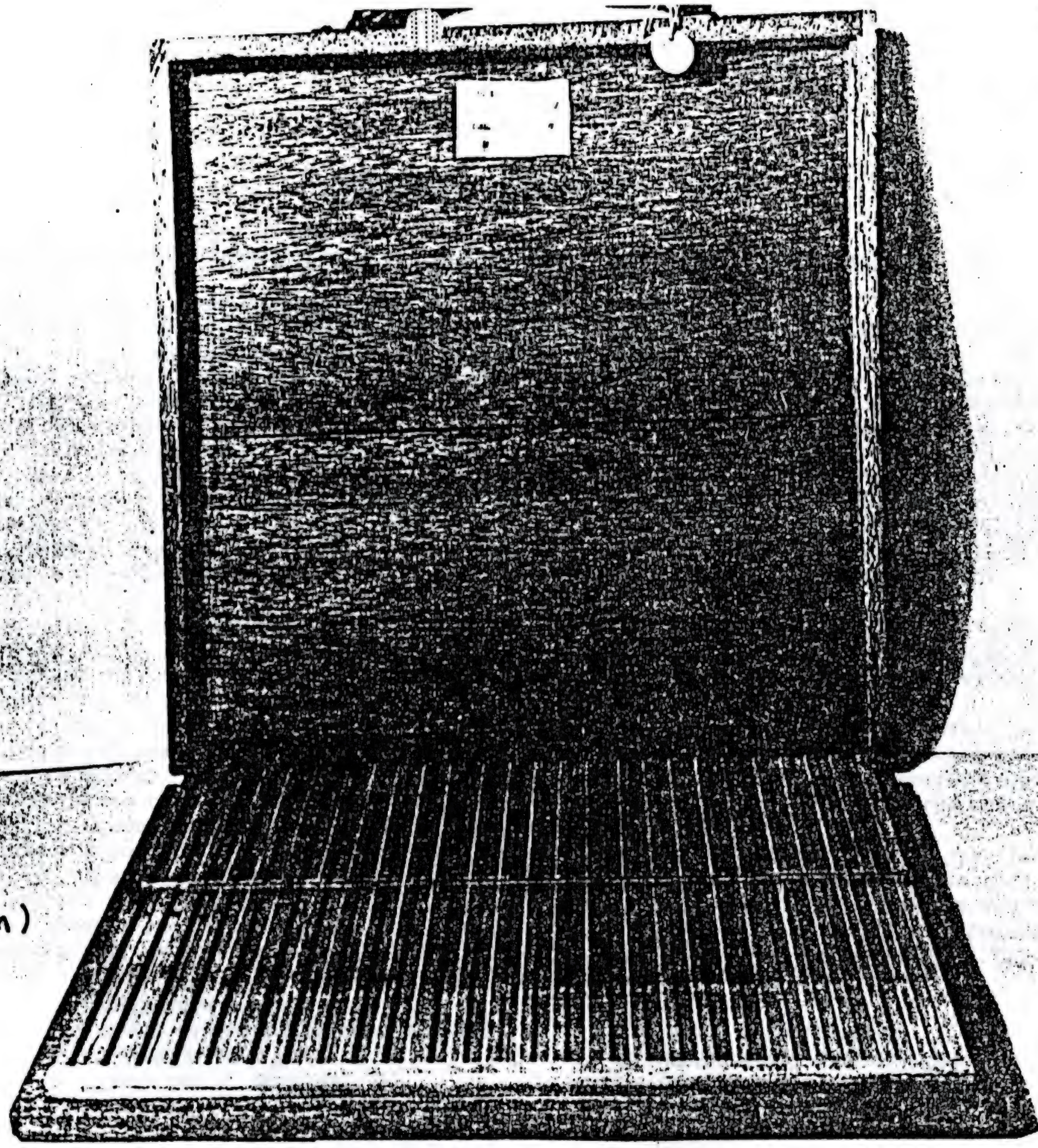
[redacted]



CIPHER DEVICE M-137
Showing change of position of parts when lever is pulled to bottom of aluminum plate.



M-138-T1
(Wooden lid closed)



M-138-T1
(Wooden lid open)

DETAILED DESCRIPTION OF CIPHER DEVICE E-138-T1

Photograph Opposite

1 - Channel
2 - Open end of channel
3 - Aluminum stop bar
4 - Metal divisions between channels
5 - Celluloid strip
6 - Double hinge
7 - Wooden board (bottom of box)
8 - Wider metal division between every five channels

Cipher Device E-138-T1 consists of an aluminum board (14½" x 14 5/8") with 25 channels (1) (¼" wide) milled into its surface; the channeled board is contained in a hinged wooden box with a leather handle. The bottom of the box is a flat wooden board (7) on which the channeled aluminum board lies and is permanently attached. The top of the box is attached to the bottom by means of a double hinge (6). This type hinge allows the box lid to be folded back and placed underneath the wooden board. With the top folded back in this manner, the board is in the position used to encipher.

The 25 channels are open (2) on only one side; the open side is at the right when the board is in position for encipherment. The other (left) ends of the channels are blocked by an aluminum stop bar (3). The metal divisions (4) between the channels are approximately 5/16 in. wide with the exception of every fifth division (8) which is approximately 7/16 in. wide. A narrow celluloid strip (5) raised from the board about ¼ in., serves as a stop for the pencil eraser when letters are being aligned.

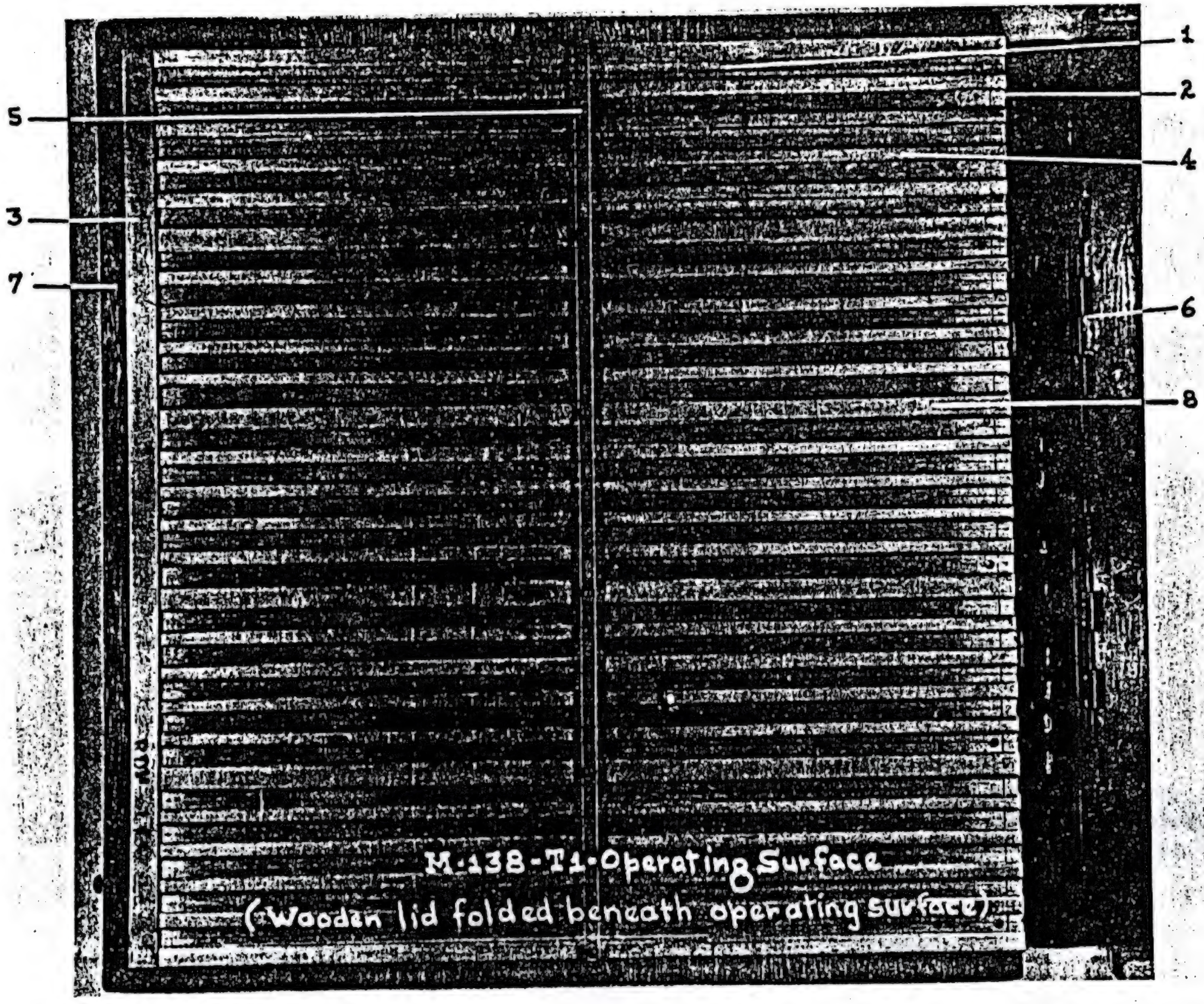
The 25 channels of the device are for the purpose of holding 25 easily-changed paper alphabet strips. Approximately 1/16 in. of the side edges of each strip fits into a tiny slot underneath the side edges of the metal divisions between the channels. This tiny slot, which admits the edges of the sliding strip, requires an extremely precise milling operation.

To encipher a message, 25 letters of plain text are aligned in a vertical column "by sliding the strips to the right as far as the celluloid stop bar will permit...The strips to the right of the celluloid bar now present a series of 25 columns of cipher letters, one of which is selected at random.... It is advisable to take a sheet of paper or ruler and set it against the column selected, to serve as a guide for the eye and prevent errors."[1] After the selected cipher-text column has been copied "the alphabet strips are then returned to their left hand positions by placing the eraser of a lead pencil on the first letter at the left of each strip and drawing the strip to the left up to the left-hand aluminum stop bar".[1] Encipherment is completed by repeating this procedure until all the plain-text letters have been aligned. Decipherment is performed by aligning the letters of the cipher text, 2 at a time, just to the left of the celluloid bar exactly as if they were plain-text letters. When 25 cipher-text letters are thus aligned the plain-text column (which is the only intelligible series of 25 letters) to the right of the celluloid bar is found and copied.

---

1. From typewritten instructions explaining intended use of Cipher Device E-138-T1; probably prepared late in 1933. AS-SCA File: Cipher Device E-138

[redacted]



M-138-T1-Operating Surface
(Wooden lid folded beneath operating surface)

[redacted]

DETAILED DESCRIPTION OF CIPHER DEVICE M-138-T3

Photograph Opposite

The third experimental model of Cipher Device M-138 (15" x 11¼") is made chiefly of red leather. The device consists of an operating surface and two wide flaps which, when closed, completely cover the operating surface. The two leather flaps are held shut by means of two snaps. On the right flap the following inscription is lettered in gold.

Confidential

CIPHER DEVICE TYPE M-138
(MODEL 3)

SIGNAL CORPS, U. S. ARMY

Register No. _____

[redacted]

Confidential

CIPHER DEVICE TYPE M-138
(MODEL 3)

SIGNAL CORPS, U.S. ARMY

REGISTER No. 2

RDM 146

4-38

DETAILED DESCRIPTION OF CIPHER DEVICE M-138-T3 (Cont.)

Photograph Opposite

1 - Pockets
2 - Cardboard strips
3 - Holder strip
4 - Gold lines

When the flaps are folded back and placed underneath the device the operating surface is exposed and the device is in operating position.

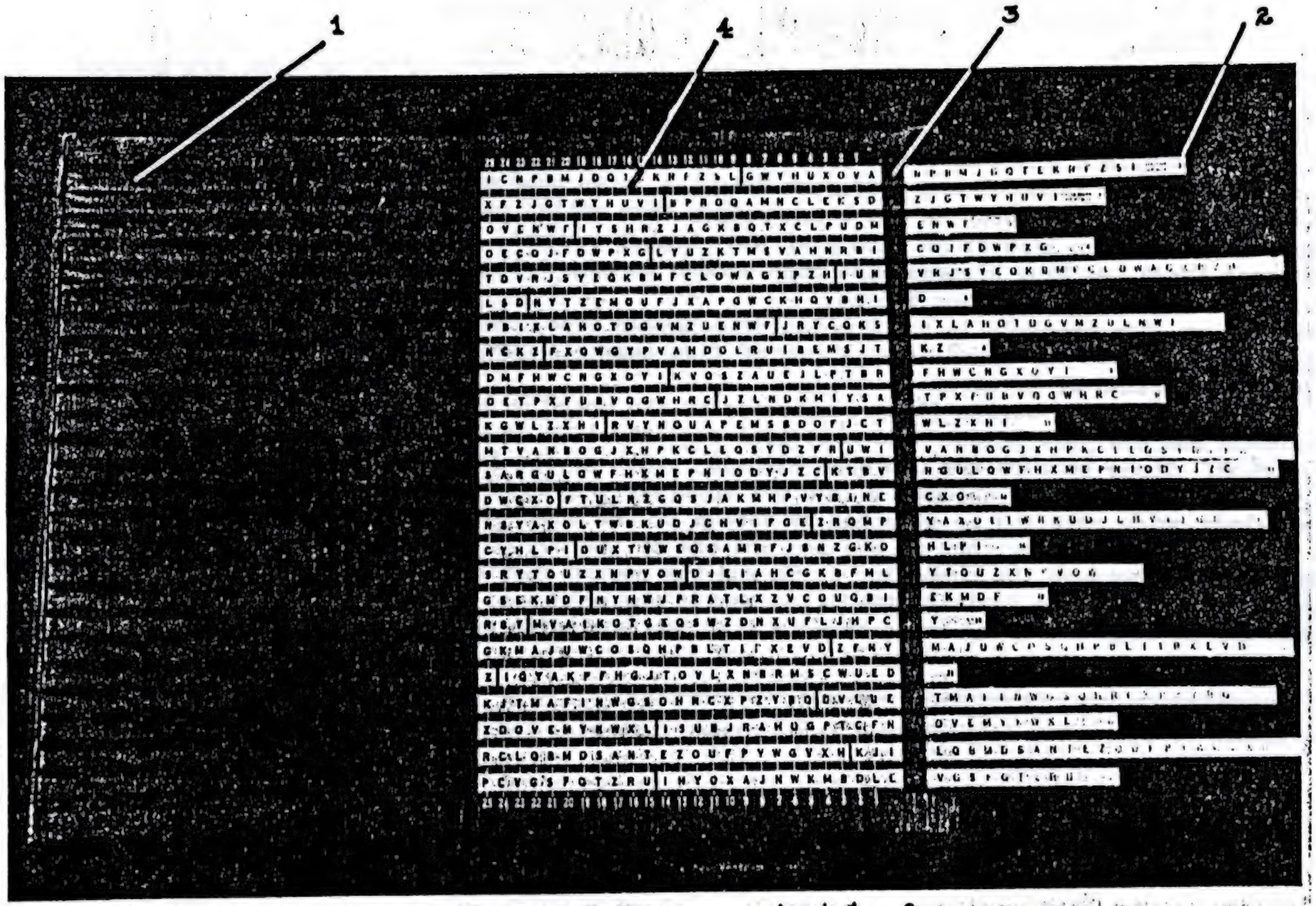
The red leather material, which covers both front and back of the operating surface, conceals a thin metal plate (15" x 14¼") which forms a strong foundation. The top surface of leather, which forms the operating surface, contains, on the left side, 25 slender leather pockets (1) (7" x 7 1/6"). They are formed by stitches of heavy black thread on both sides of each pocket. These 25 pockets hold cardboard strips (2) each printed with a random-mixed alphabet and a repetition of it.

On each strip, the random alphabet and its repetition are separated in the center of the strip by a heavy black line. At the right end of each strip is the number of the strip in the series; the strips are numbered from 1-25. On the right end of the first three strips is the following information: On strip number one is the number of the alphabet set; on strip number 2 is the name of the device; on strip number 3 is the register number of the alphabet set.

Near the right edge of the operating surface, a red leather holder strip (3) (width: 3/8") is attached to the operating surface in a vertical position. The right ends of the alphabet strips slide under this leather holder strip. Between each horizontal alphabet strip, the vertical holder strip is stitched to the leather surface. This stitching aids in holding the alphabet strips in a straight horizontal line. The left edge of the leather holder strip provides a guide for aligning plain text when enciphering and cipher text when deciphering.

Twenty-five thin gold lines (4) (length: 10 1/8"), positioned at a distance of ¼ in. from each other, extend from near the top (within 9/16 in.) of the operating surface to near the bottom (within 9/16 in.). These gold lines are numbered, right to left, from 1-25.

The method of operation was, in general, to align 25 plain-text letters in a column and choose at random a cipher-text column from among the remaining 25 generatrices. This operation was repeated as many times as necessary to complete encipherment. Apparently, the intention was to align the plain text at the left of the leather-holder strip in such a position that the first gold line bisected the letter just to the left of the plain-text letter. Such positioning insured that each of the 25 letters left of the plain-text letter on each strip was bisected by one of the 25 gold lines. Any number above or below lines could then be chosen at random and the column of letters designated by the number chosen would constitute the cipher generatrix. To decipher, the procedure was reversed, that is, the cipher text letters were aligned at the left of the leather-holder strip and the plain text found among the columns numbered in gold from 1-25.



M-138-T3 Operating Surface
(Flaps folded back)

~~SECRET~~

DETAILED DESCRIPTION OF CIPHER DEVICE H-138-T4.

Photograph Opposite

1 - Alphabet strip in channel
2 - Space, stained black, between every five channels
3 - Numbering strip
4 - Guide rule
5 - Stop screws

Cipher Device H-138-T4 consists of a thin aluminum board (14 7/8" x 12¼") on which are mounted horizontally, 25 aluminum channels (14 1/8" x 5/16"). These channels hold paper strips containing random-mixed alphabets (1). The aluminum board curves upward ¼ inch at top and bottom. The back of the board is padded with a piece of green felt.

The channels of the T4 model are different from the later used models in that the channels are constructed separately and mounted on the board rather than milled into the surface. The edges of the channels are curved up 1/16 of an inch over the channel surface. This curvature of both edges of each channel forms two tiny grooves just high enough to permit the edges of the paper alphabet strips to fit into them and to slide freely.

Between every five channels is a space (2) 3/16 inches wide, which is stained black. These dark spaces effectively divide the board into groups of five channels each, thereby aiding the eye in aligning and copying a column of letters.

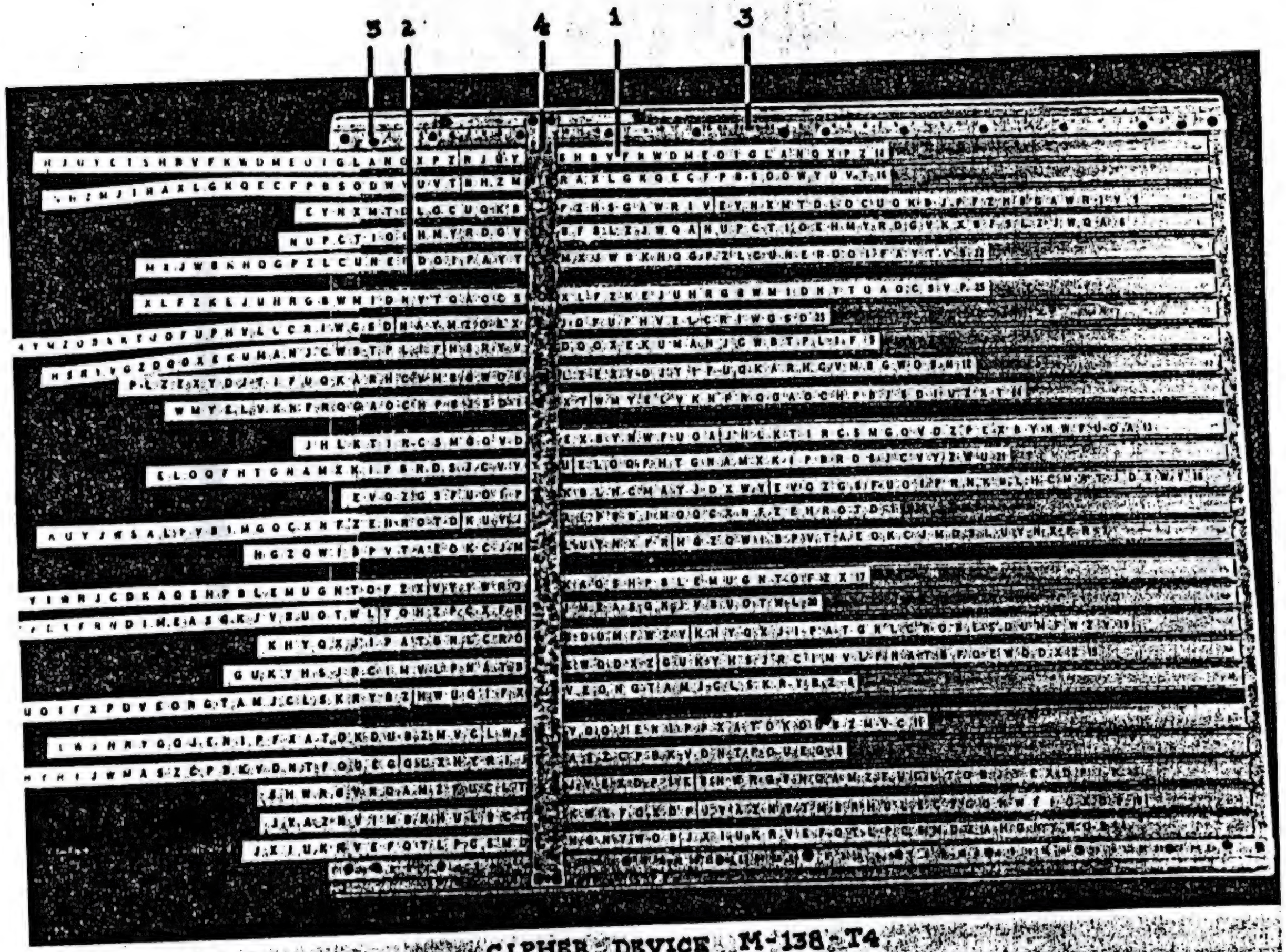
Two aluminum numbering strips (3) are attached to the board by means of screws, one just above the 25 channels and one just below. The numerical sequence 1-26 is twice engraved on each of these aluminum strips. These numbers are the same distance apart as the letters on the alphabet strips, thus providing a means of numbering columns of letters vertically aligned on the board.

An aluminum guide rule (4) is attached by screws to two short narrow aluminum slide pieces. Each of these short aluminum pieces (one at the top and one at the bottom of the board) slide in a groove formed by the space between the numbering strip and the upward curving edge of the board. This arrangement enables the operator to position the slide beside any column of letters. Four stop screws (5), one at each end of each numbering strip, form a stop for the guide rule.1

---

1. The method of operation is explained on the page following this photograph.

~~SECRET~~



CIPHER DEVICE M-138-T4
(CIPHER DEVICE M-138-T2 with improvements)

[redacted]

METHOD OF OPERATION

To encipher a message, first push the guide rule to the left as far as the stop screws will permit. Then align the plain-text letters in a column just to the left of the guide rule; this will bring the letters to a position just beneath the number 1 of the numbering strip. Choose at random any number from 2-26 on the numbering strips, and place the right edge of the guide rule adjacent to the number selected. (Use only the first series of numbers located at the left of the numbering strip; some of the columns indicated by the second series of numbers will be incomplete.) Care must be exercised never to choose column 1 in the center of the board; this column is the plain-text generatrix. The column chosen at random by positioning the guide rule, as described above, is the cipher-text column; copy it in five-letter groups. Then repeat the above procedure as many times as necessary in order to complete encipherment of the message.

To decipher a message reverse the procedure, that is, align the cipher-text letters beneath the number 1 and find the resultant plain-text column among the numbers 2-26.

It is also possible to encipher by aligning the plain-text letters (from the left-hand alphabet on the strips) under the number 1 in the center of the board and then choosing the cipher-text column at random from among the columns to the right of the plain-text alignment. This method has the advantage of throwing the repeated plain-text column so far to the right that the stop screws make it impossible to place the guide adjacent to it. This feature gives this second method the advantage of guarding against possibility of inadvertently copying the repeated plain-text column.

[redacted]

[redacted]
C O P Y

THE SIGNAL CORPS BOARD
FORT MONMOUTH, NEW JERSEY

April 20, 1934

REPORT ON
SIGNAL CORPS BOARD CASE NO. 193
CIPHER DEVICE, TYPE M-138
File OCSigO 413.6 (M-138)

DIRECTIVE: 8

"WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

OCSigO 413.6 (M-138) March 7, 1934

Subject: Cipher Device, type M-138.

To: President, Signal Corps Board, Fort Monmouth, N.J.

Signal Corps Board Case No. 193.

1. There are being sent you this date by express three different models of a proposed new cipher device to which the type number M-138 has been tentatively assigned by the Chief Signal Officer. The cryptographic principle of these devices is essentially identical with that of Cipher Device, type M-94, except that they employ paper strips bearing easily changeable alphabets which are to be slid horizontally in channels, in cryptographing or decryptographing messages. It is desired that you service test these models and submit recommendations for the consideration of the Chief Signal Officer as to which model is deemed most practicable for military use.

2. It is proposed to adopt this as a cryptographic device in tactical units down to and including division message centers, as an auxiliary means of secret communication between holders of Army Field Code. If successful, it may eventually replace Army Field Code altogether.

3. Tests to establish the degree of cryptographic security afforded by such a device have been made. They have

[redacted]
C O P Y

demonstrated that the changeable alphabets of this type of device afford a very much higher degree of cryptographic security than do the unchangeable alphabets of Cipher Device, type M-94. A single fairly long message cryptographed by means of the latter device, the alphabets of which are presumably known to a potential enemy, can be solved in from three to forty-eight hours, and a set of messages all in the same key can be solved in less than twelve hours under favorable conditions. However, in the case of Cipher Device, type M-138, tests have indicated that, given a staff of six competent cryptanalysts, working on traffic totaling 3,000 five-letter groups all in the same key (sequence of alphabets) solution cannot be reached in less than one week's concentrated effort. Consequently, if the change in key is made sufficiently often so that not more than this number of groups is enciphered in any one key, a set of alphabets may be employed with safety for a considerable number of days or until the alphabets have been compromised by capture or other means.

4. a. Models 1 and 2 are practically identical, both using alphabet strips cut out from sheets of heavy bond paper similar to sample enclosed herewith, labeled Exhibit 1. These sheets could be printed in the field, and issued to holders, who could cut them into strips by a razor blade or sharp knife. The cuts must, however, be extremely accurate and for this reason it may be necessary to develop a cutter which will automatically cut the strips apart, as per Exhibit 2. This matter is being investigated by the Chief Signal Officer and at present no difficulties are foreseen in this direction. Should an automatic cutter be deemed necessary, the cutting could be done at the printing plant, as in Exhibit 2, so that the strips would remain together in the sheet until actually ready for insertion in the device.

b. Tentative instructions for the use of models 1 and 2 accompany this letter and are marked Exhibit 3. Sliding strips have already been inserted in the channels, and set up to the same key.

c. Model 3 is identical with a model recently adopted as standard by the Navy. This model uses alphabet strips of cardboard in channels made in a leather holder. Accompanying this letter is a copy of the instructions (Exhibit 4) and a set of strips (Exhibit 5) as issued by the Navy Department for use with their device. These instructions and alphabets are now in actual service in the Navy and it is directed that all precautions be exercised in their handling, to prevent their loss or compromise. They must be returned as soon as this service test is completed.

d. The strips of the Navy model are partially cut by a special machine at the Government Printing Office; a sharp knife or razor blade will separate them.

e. A factor to be considered is the comparative costs of replacement alphabets in the case of model 1 or 2 as against model 3. The paper stock for Exhibit 1 is much cheaper than that for Exhibit 5; the cutting of the former is possible as a single operation at very slight cost per sheet by means of a set of rotary-disk knives keyed to one shaft; the cutting of the latter is a much more costly operation since the whole sheet must be advanced 25 times, once for each strip, and this is a slow, hand-feeding operation.

5. The following points are specifically presented for your study and determination:

a. Speed of operation of Models 1, 2 and 3 as compared with Cipher Device, type M-94 in:

(1) Setting up the device to a new key
(2) Cryptographing and decryptographing

b. Speed of operation of Model 2 as compared with Model 3 in:

(1) Setting up the strips to a new key
(2) Cryptographing and decryptographing

c. Relative susceptibility to errors in the case of Models 1 or 2 compared with Model 3.

d. Relative ruggedness and durability of Models 1, 2, and 3 under field conditions.

e. Relative ease in storage and transportation and resistance to damage in handling of Models 1, 2, and 3.

6. Memorandum receipt covering these models and accompanying exhibits is enclosed. It is requested that upon receipt of this material this receipt be completed and returned without delay.

7. It is requested that this service test and report

thereon be submitted to the Chief Signal Officer by April 15, 1934.

By order of the Acting Chief Signal Officer:

Enclosures:
Exhibits 1-5 incl.
Memo Receipt covering above.

/s/ G. L. Van Deusen,
Major, Signal Corps
Executive."

PROBLEM PRESENTED:

To determine which of the models 1, 2 and 3 submitted for test is the most satisfactory replacement for the Cipher Device M-94, and meets the needs of the military service under field conditions.

FACTS BEARING ON THE CASE:

The board collaborated with Major William F. Friedman, Signal Corps Reserve, War Department Cryptanalyst, and 1st Lieut. Mark Rhoads, Signal Corps, and their ideas and opinions were considered. The tests outlined in paragraph 5 a, b, and c, of the directive letter were made by a group of one noncommissioned officer and four men who were assigned for this duty, under the direction of 1st Lieut. Mark Rhoads, Signal Corps. Each man was assigned a different device each day, time was taken for the start and finish of encipherment, decipherment, and the setting up of key words. Comparisons were made by individuals, that is, the results of each man's work on all four devices were used for direct comparison. This was done in order to eliminate the personal element of natural speed or ability, or the lack of it. Specific results were as follows:

Regarding paragraph 5 a (1) of the directive letter, setting up device to new key:

M-94 can be set up almost 3 times as fast as Model 1
M-94 can be set up twice as fast as Model 2
M-94 can be set up slightly less than twice as fast as Model 3

The reason for this loss of time is due to the difficulty of starting the strips into the channels.

Regarding paragraph 5 a (2), cryptographing and decryptographing:

Models 1, 2 and 3 are about equal in speed of operation, and are about 1/3 faster than the M-94, both in cryptographing and decryptographing. No especial difficulty was experienced due to the necessity of reading vertical columns of letters in models 1, 2 and 3 as against reading horizontal lines of letters in the M-94.

Regarding paragraph 5 b (1), setting up the strips to a new key:

Model 3 is slightly faster (about 1/8) than Model 2.

Regarding paragraph 5 b (2), cryptographing and decryptographing: Speed of operation almost exactly equal between models 2 and 3.

Regarding paragraph 5 c, relative susceptibility to errors in the case of models 1 or 2 compared with model 3: Practically no difference.

With reference to paragraph 5 d and e, relative ruggedness and durability of models 1, 2 and 3 under field conditions, the following points have been noticed:

Models 1 and 2 are more rugged than model 3; in fact model 1 is too rugged and carries unnecessary weight. The strips used with model 3 (Navy) are brittle and liable to be bent when being returned "to battery". The sewing on the pockets and guide strips of Model 3 is liable to rot out with excessive moisture which might also cause general warping of the entire device. The Navy instructions for model 3 call for the use of a blunt-edged paper cutter to enlarge the openings of the guide strips so as to permit free motion of the sliding strips. This is impractical from the Army standpoint. In practical usage the pointed end of a pencil would replace the above instrument and the slightest carelessness would result in ripping out the stitches.

The channels of model 2 are less rugged than those of model 1, and could possibily be bent down by dropping a heavy object on them so as to prevent the free passage of the strips, but even so they could be pried up with a knife or screwdriver.

The board believes that the part of the device containing the block and channels of model 2 is satisfactory except for the following:

The right end of the channels should be modified to facilitate putting the strips into the channels.

The channel block should contain, as part of it, a device consisting of a slide and marker for the purpose of reading the vertical columns of letters, thereby eliminating the ruler which, as a loose piece of equipment, is likely to be lost or its setting disturbed.

CONCLUSIONS:

That the channel block and channels of a type similar to model 2, protected by a folding cover of waterproof webbing, or some durable fabric other than leather, similar to the cover of model 3 (Navy), be adopted.

That the cover be arranged so that it can be securely fastened.

That the paper on which the alphabets are printed be light enough to permit of easy sliding into the channels, be of light green color with letters in black, and be without glaze.

That all metal parts of the channel block and channels be of dull finish.

RECOMMENDATIONS:

The board recommends that:

1. The Signal Corps Laboratories, Fort Monmouth, New Jersey, be directed to develop, as part of Project No. 86, a model similar to that of model 2 and incorporating the ideas in accordance with those contained in the CONCLUSIONS of this report.

2. Models 1, 2 and 3, together with all descriptive matter and alphabets, be turned over to the Signal Corps Laboratories for use in making up the model referred to above.

CONCURRENCES:

I concur in the above report.

WM. R. BLAIR,
Major, Signal Corps,
OC, Signal Corps Laboratories,
Member.

/s/ A. S. COWAN,
Colonel, Signal Corps,
President.

/s/ FRED G. MILLER,
Captain, Signal Corps,
Member and Secretary.

/s/ O. S. ALBRIGHT,
Lt. Colonel, Signal Corps
Asst. Comdt., The Signal School, Member.

/s/ H. C. INGLES
Major, Signal Corps,
CO, 51st Signal Battalion
Member

Concurred in but not signed due to absence from station.

THE SIGNAL CORPS BOARD
FORT MONMOUTH, NEW JERSEY.

June 7, 1934

REPORT ON
SIGNAL CORPS BOARD CASE NO. 199
CIPHER DEVICE, TYPE M-138-T4
File OCSigO 413.6 (M-138-T4)

DIRECTIVE:

"WAR DEPARTMENT
Office of the Chief Signal Officer 8
OCSigO 413.6 (M-138-T4) Washington May 14, 1934

Subject: Cipher Device, type M-138-T4

To: President, Signal Corps Board, Fort Monmouth, N. J.

Signal Corps Board Case No. 199

1. Reference is made to Signal Corps Board Case No. 193. There will be turned over to you within the next ten or fifteen days a single exemplar of Cipher Device, type M-138-T4. This model will have been developed by the Signal Corps Laboratories in accordance with recommendation No. 1 of your report on Case No. 193.

2. It is proposed to adopt Type M-138-T4 as a cryptographing device in tactical units down to and including division message centers, as an auxiliary means of secret communication between holders of Army Field Code. It is desired that you consider and test this model with this point in mind.

3. The following points are, in addition, specifically presented for your study and determination.

a. Relative ruggedness and durability of type M-138-T4 as compared with the models studied in connection with Case No. 193.
b. Relative ease in storage and transportation and resistance to damage in handling M-138-T4 as compared with the same points with regard to the models studied in connection with Case No. 193.

~~SECRET~~

COPY

4. It is requested that this service test and report thereon be submitted to the Chief Signal Officer by June 15, 1934.

By order of the Chief Signal Officer:

(S) G. L. Van Deusen
G. L. Van Duesen, (sic)
Major, Signal Corps,
Executive."

ASSIGNMENT:

To consider and test model of Cipher Device, type M-138-T4.

RECORD AND PROCEDURE:

The model of Cipher Device, type M-138-T4, turned over to the Board by the Signal Corps Laboratories, consisted of the base of model type M-138-T2, the sides of which had been cut down smooth, and to which had been added:

a. A felt backing,
b. A filler strip of material having the same thickness as the material used in the guides for the alphabet,
c. A straight edge slide, and
d. A strip of aluminum carrying numbers to facilitate the setting of the slide.

In addition to this, the upper metal surfaces were sanded in order to avoid light reflection and make the use of the device easier on the eyes of the operator. It is understood that the Aluminum Company of America makes a material having a smooth dead surface which might possibly be better than the somewhat roughened sanded surface of the model. Samples of this material have been requested by the Signal Corps Laboratories but have not yet been received.

A protective carrying case for the device was provided. It was explained by a Laboratories' representative that this case was gray in color rather than olive drab as desired by the Board,

~~SECRET~~

COPY

because the company making the case had no olive drab material in stock. This material is stocked by the roll, and the Laboratories deemed it advisable to have the single model made of the gray material rather than go to the expense of providing a roll of the olive drab material. Olive drab material may be specified when the device goes into production. It was further explained by the Laboratories that thru error the manufacturer of this case placed the zipper fasteners on the side rather than on the end of the case as they had been instructed to do. The construction of the device is such that it slides into the case endwise better than sidewise. The model was accepted with the fasteners on the side because of the lack of time to have a new model construc%ed. When the device goes into production it will be a simple matter to specify the zipper fasteners on the end instead of on the side as in the present model.

In order to further facilitate resetting the strips, one strip (No. 17) was slightly tapered on the left end. This taper was formed by removing the corners from the left end of the strip. The material removed from each corner was approximately 1/16" wide by 3/16" long. This slight taper, together with the filler strip listed in "b" above, speeds up the resetting of the strips materially.

This model was turned over for test to the same group that made the tests in connectinn with Signal Corps Board Case No. 193. In his report of service test of this model, Lieut. Rhoads, officer in charge of test group, repoets:

a. The time required to cryptograph and decryptograph was appreciably reduced. The best time on any of the previous models was an average of 2 minutes per line, whereas the time on this model averaged 1.7 minutes per line.

b. As to the matter of errors, in the previous models from two to seven errors were made in twenty lines of text, whereas in the present model no errors were made.

c. The changing from the box-like arrangement opening with hinges to the present one of providing a carrying case is in my opinion much more satisfactory from the viewpoint of both portability and operation. The case would be improved by putting the zipper fasteners on the end rather than on the side.

~~SECRET~~

COPY

CONCLUSIONS:

The Board concludes:

a. That the operation of the device has been considerably improved by the changes that have been introduced in the model T4.

b. That the present model, including its carrying case, is more rugged and durable than any of the models tested in connection with Case No. 193.

c. That the model T4 can be more conveniently stored and transported than any of the previous models, and that the carrying case with this model forms a better protection for the device than was provided by any of the protective means supplied with models tested in connection with Case No. 193.

RECOMMENDATIONS:

The Board recommends:

a. That a cipher device similar to the model type M-138-T4 be adopted as standard for the uses specified in the above directive.

b. That in future production of this equipment the carrying case be olive drab in color and have the zipper fasteners on the end rather than on the side.

c. That the alphabet strips be slightly tapered on the left end to facilitate resetting.

CONCURRENCES:

I concur in the above report.

/s/ H. C. INGLES,
Major, Signal Corps
CO, 51st Signal Battaltion
Member.

/s/ A. S. COWAN,
Colonel, Signal Corps,
President.

/s/ WM. R. BLAIR,
Major, Signal Corps
OC, Signal Corps Laboratories,
Member and Acting Secretary

/s/ O. S. ALBRIGHT,
Lt. Colonel, Signal Corps
Asst.Comdt., The Signal School, Member.

~~SECRET~~

COPY

~~SECRET~~

DETAILED DESCRIPTION OF CIPHER DEVICE M-138

Photograph Opposite

1 - Cylindrical rod divisions between channels
2 - Dark cylindrical rod division (One between every 5 channels)
3 - Channel
4 - Rectangular metal strip
5 - Guide rule
6 - Rod on which guide rule slides
7 - Rubber leg
8 - Metal rod support

Cipher Device M-138 consists of an aluminum board (16" x 11") on which are mounted, horizontally, 26 slender cylindrical rods (1). The rods are 5/8" apart and extend from one side of the board to the other. The spaces between the rods form 25 channels (3) in which paper alphabet strips may be slid. Every fifth cylindrical rod (2) is dark; this feature effectively divides the board into groups of five channels each, thereby aiding the eye in aligning and copying a line of letters.

Along the edges of the channels on each side of the board is a rectangular metal strip (4) which rests on top of the cylindrical rods, thus forming a slot for inserting and sliding the alphabet strips. The base of the rectangular metal strip is grooved at the points where it fits over the cylindrical rods so that although the rods are 1/8" in diameter, the slot between the rectangular strip and the board is only 1/16" high.

The cylindrical rods are fastened to the aluminum board by means of rivets. Four rivets hold each rod; two that go through the metal strip at the ends of the channels as well as through the rod and board, and two that go through the rod and board.

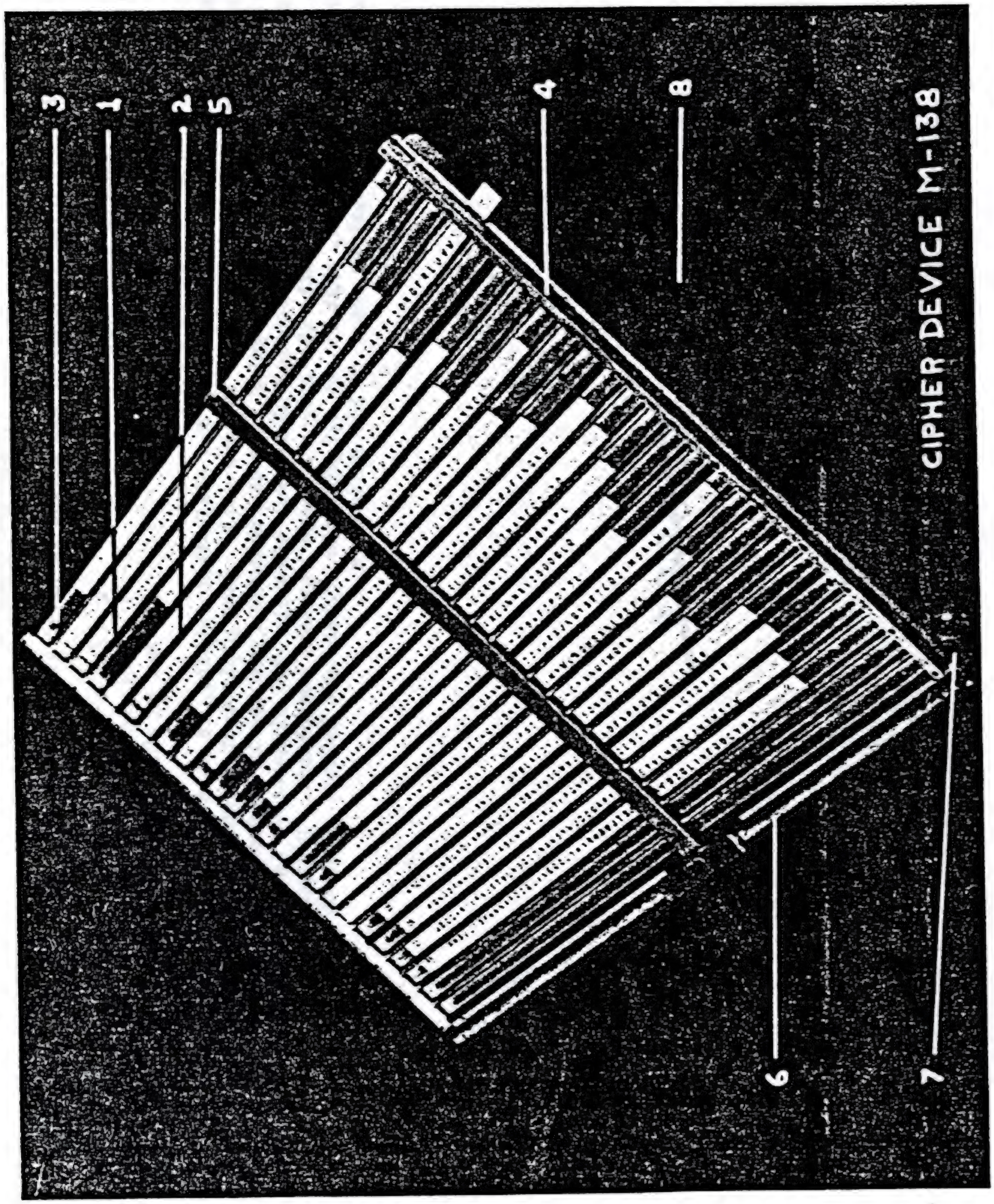
The upward curving of each cylindrical rod forms a tiny groove, at the base of each channel, into which the edges of the paper alphabet strip fits. This groove is just high enough to permit one alphabet strip to fit into it.

A guide rule (5) which slides along a rod (6) at the bottom of the board, aids in copying a column of letters.

When the device is laid flat, it rests on four small rubber legs (7). It will also stand at about a 45° angle by means of a metal rod support (8). The rod support is attached to the base of the board by a small rectangular block; a groove in the base of the block grasps the rod; a screw, which penetrates the block and the board, holds the block and thus the rod to the board. The rod may be turned in the groove so that it will either lie flat against the board or extend to support the board at an angle. The long section of the curved rod support is covered by rubber tubing to protect the surface on which it rests.

The method of operation is given in Tab 23.

~~SECRET~~


3
1
2
5
4
8
CIPHER DEVICE M-138
6
7

~~SECRET~~

METHOD OF OPERATION OF CIPHER DEVICE M-138

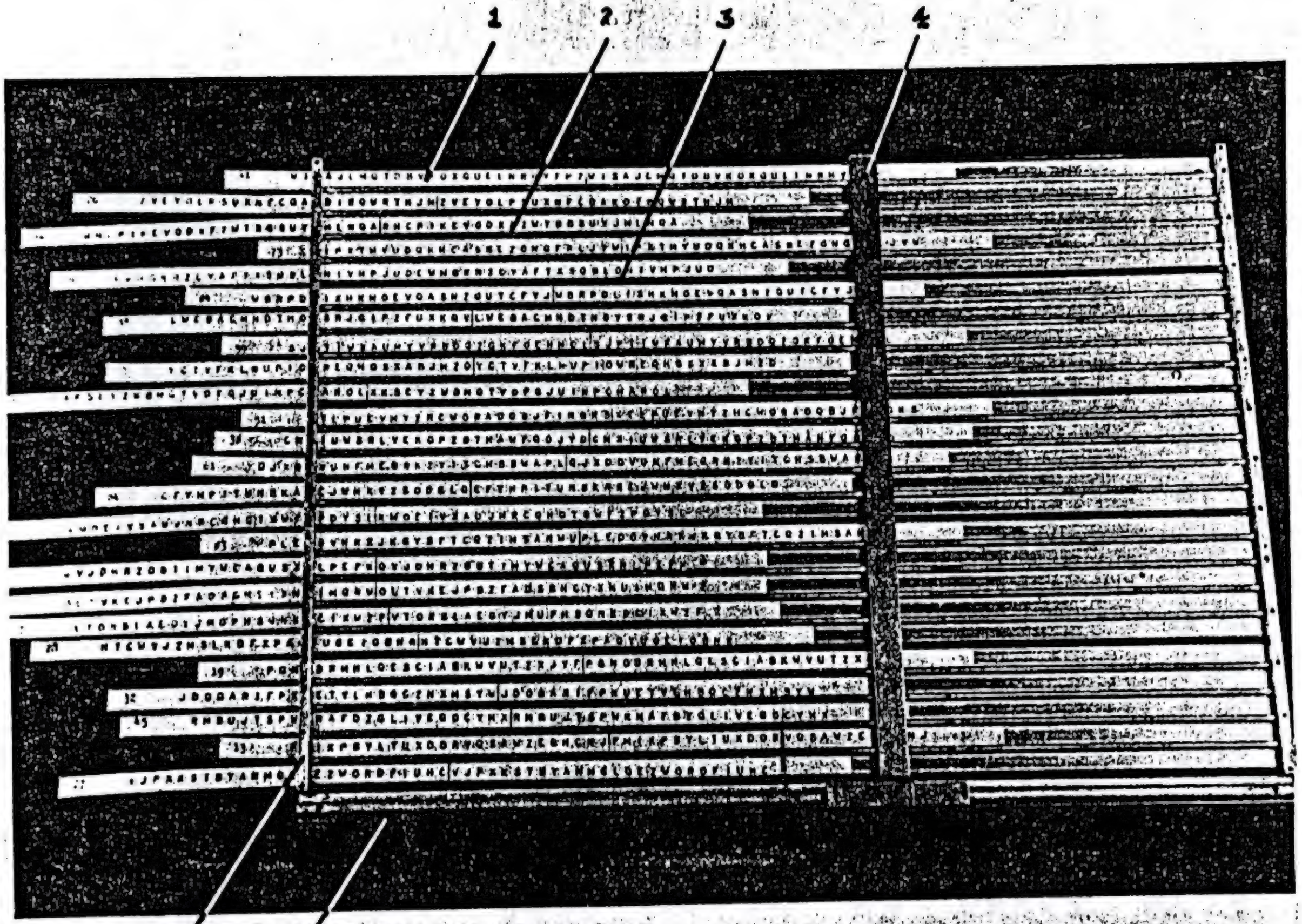
Photograph Opposite

(Detailed description of the device is given in Tab 22)

1 - Channel with alphabet strip
2 - Cylindrical rod
3 - Dark cylindrical rod
4 - Guide rule
5 - Rectangular metal strip
6 - Rod on which guide rule slides

The method of operation is to align the plain-text letters, 25 at a time, in column adjacent to the metal strip at the left end of the channels. (See plain-text alignment). The cipher-text letters are chosen by sliding the guide rule at random and placing it adjacent to any other full column of letters (except the repeated plain-text column). The cipher-text letters are then copied and the operation repeated until the entire message has been enciphered. Decipherment is performed by reversing the procedure, that is, by aligning the cipher-text letters adjacent to the left strip and finding the plain text by means of the guide rule.

~~SECRET~~



CIPHER DEVICE M-138

Draft Specifications for a Rotary Cutting Machine

These specifications are intended to cover a reliable rugged cutting machine to cut semi-cardboard sheets into 65 strips. The width of each strip is to be .3475" and this width is to be maintained in the finished product to within .0015".

The cutter knives are to be circular and approximately 2⅛" to 2½" diameter, beveled on one edge only. There will be 26 of these rotary knives mounted on a sturdy spindle not less than 1¼" diameter and geared (gears guarded) to a lower spindle of the same diameter and with the same number of rotary knives only beveled in opposite direction.

The knife material is to be not more than .125" thick. the knives must be interchangeable; the space between knives is to be taken up by interchangeable spacers.

The knives must cut good clean equal-spaced strips, and be made of the best quality high speed steel for the purpose. The machine shall be so arranged that the two sets of cutting knives may be separated to permit of inserting into the machine the material to be cut, and then closed while the cutting is accomplished; they must then be again separated near the finish of the cut, so that the material may be removed, leaving the strips so cut fastened at each end. This is done so that the strips, although cut apart may be left attached to the sheet for shipment and parted when ready for use by simply cutting off both ends with ordinary hand shears.

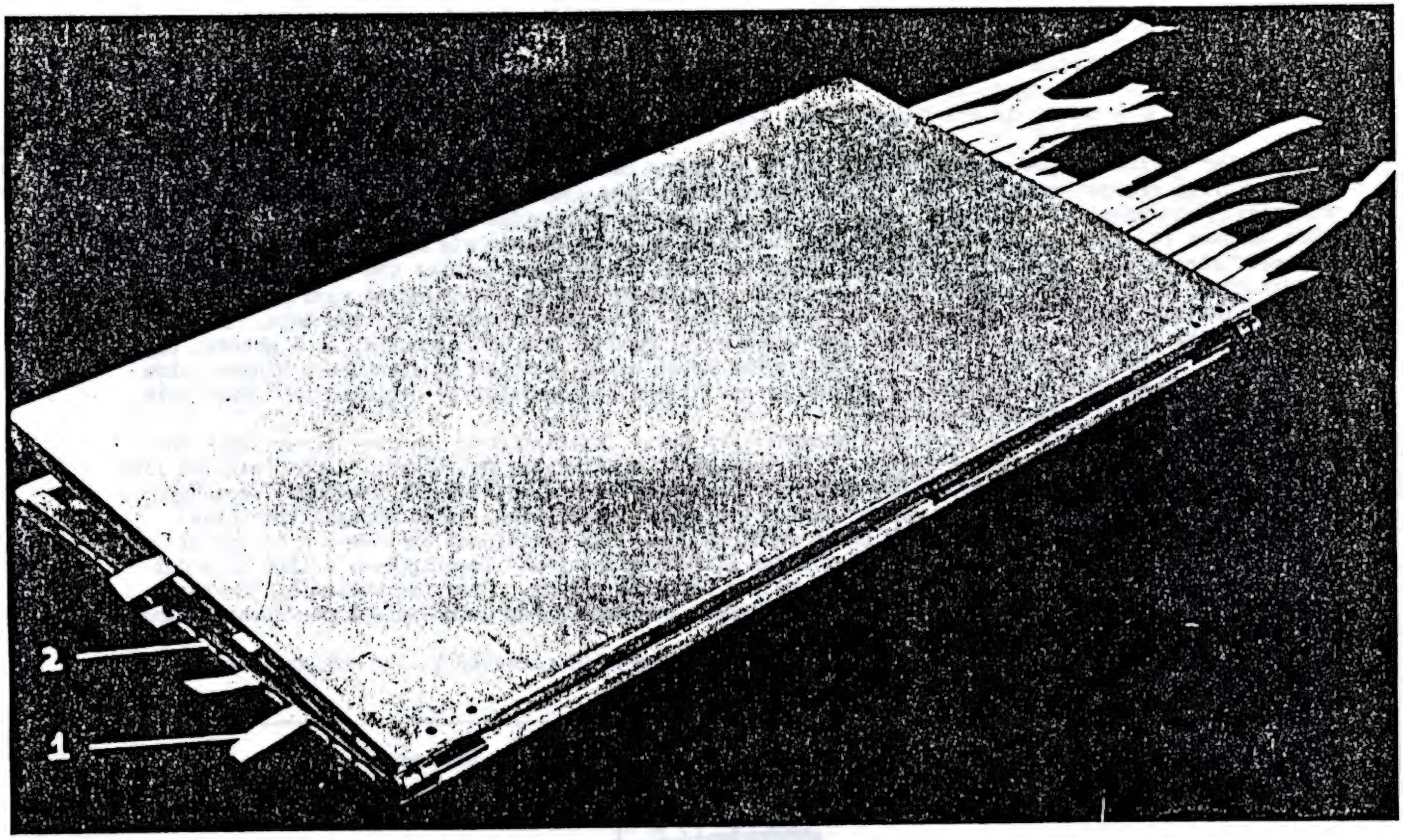
The point of start and stop of the slitting must be automatic and so arranged as to permit cutting strips of varying lengths by lengthening or shortening the table upon which the paper stock is placed for feeding into the machine.

The machine is to operate with but one hand crank, is to be rugged and simple in design.

The bidder must submit with his bid two sets of prints or drawings showing the general design of the machine he proposes to furnish. The government reserves the right to reject any or all designs which in its opinion will not perform in a satisfactory manner the work for which this machine is intended.

cosigo
June 20, 1936

C O P Y



CIPHER DEVICE M-138-A
(Closed)

DETAILED DESCRIPTION OF CIPHER DEVICE M-138-A

Photograph Opposite

1 - Channel
2 - Side border
3 - Double division between every five channels
4 - Groove in which guide rule slides
5 - Guide rule
6 - Flat metal portion containing inscriptions
7 - Vertical RED "Do not copy" line
8 - Hinge for closing board

Cipher Device M-138-A consists of a hinged aluminum board (14 5/8" x 15 11/16") into which are milled thirty grooved channels (1). These channels are designed to hold changeable paper strips containing random-mixed alphabets. The channeled board is surrounded by a metal border. The two side borders (2) rest upon the edges of the channels, thus forming thirty slots through which paper alphabet strips pass when sliding in the channels. The top border contains the following inscription: SIGNAL CORPS U. S. ARMY - CIPHER DEVICE M-138-A. The lower border has engraved upon it the name of the manufacturing company, which was Kidin Metal Goods, the order number, and the date. At the bottom of the channeled board, between the lower metal border and the channels, is a groove, (4) 5/8" wide. In this groove is a small rectangular metal block to which is attached a hinged guide rule (5). The sliding of this block in the groove allows the operator to position the guide rule at will. The guide rule is removable.

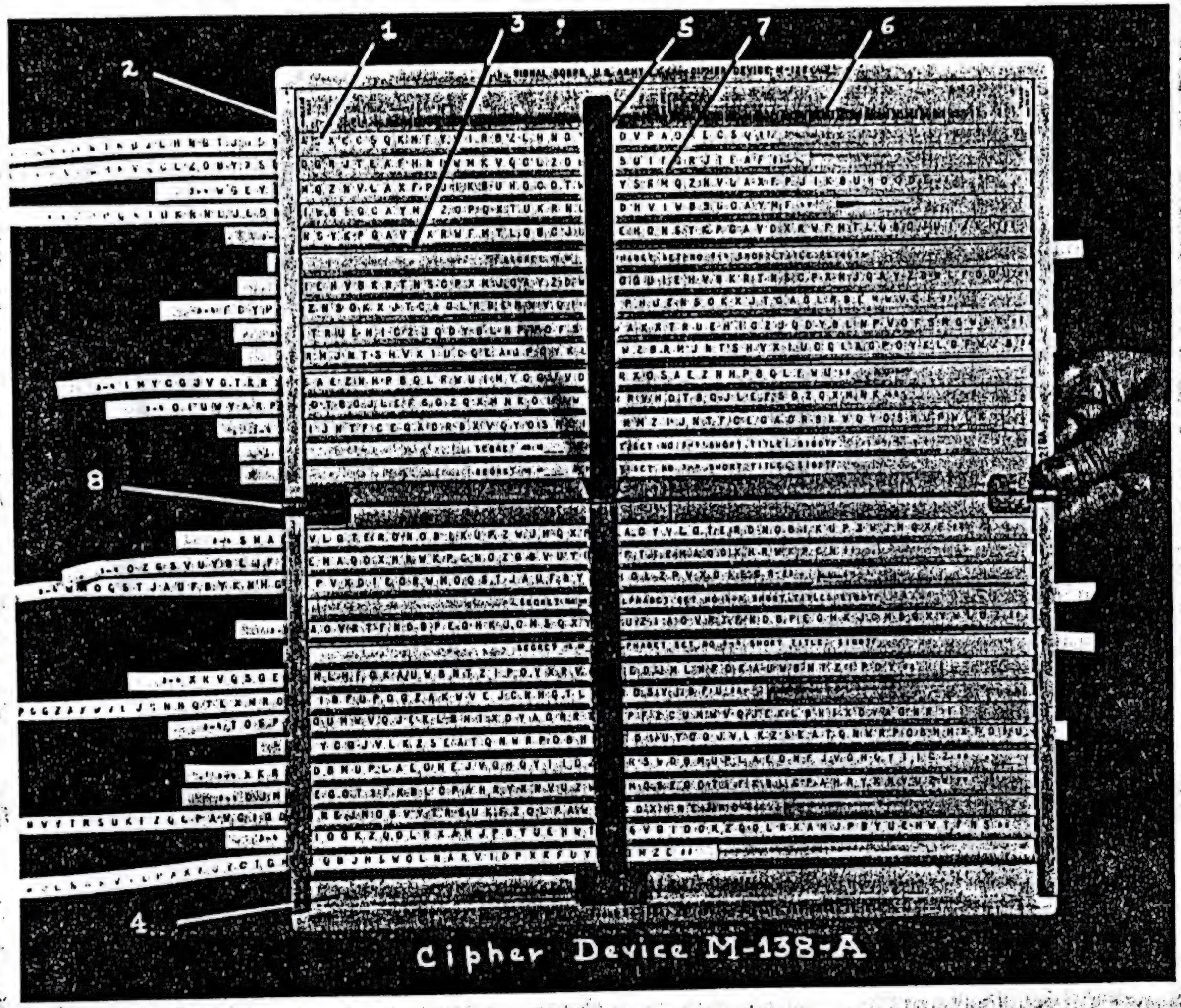
On a flat metal portion above the channels are three inscriptions: At the extreme left and extreme right is written "Clear Text"; in the center is written "Do not copy". A vertical red line (7), broken because it appears on the horizontal metal divisions between the channels, runs down the center of the board directly under the "Do not copy" inscription. Just beneath the three inscriptions is a series of dots and short vertical lines, so positioned that when a column of letters on the alphabet strips is aligned under either "clear text" inscription, a line or a dot will be directly above a column of letters on the alphabet strips. Near the bottom of the board, the division between the last channel and the groove containing the guide-rule block shows a similar series of lines and dots.

The board is made in two equal sections and is hinged (8) directly in the center to enable the operator to close the board.[1]

---

1. The method of operation is explained on the page following this photograph.

SECRET



Cipher Device M-138-A

~~SECRET~~

METHOD OF OPERATION

The method of operation is as follows: To encipher a message, align the first 25 letters of plain text under either short line above which is written "clear text". Choose a cipher-text column at random by sliding the guide rule and placing it adjacent to any other full column of letters except the one inscribed "Do not copy". The red line which emphasized this column from top to bottom will aid the operator in avoiding it. Repeat the above precedence as many times as necessary to completely encipher the message, provided the message does not exceed the length limitation (see page 79), in which case it will be divided into parts.

To decipher, align the cipher-text letters in a column beneath either one of the "clear text" inscriptions and find the plain-text column.

~~SECRET~~

DETAILED DESCRIPTION OF CIPHER DEVICE M-138-A (WOOD), (Short title: SIGWOO)

Photograph Opposite

1 - Channel
2 - Alphabet strip
3 - Horizontal divisions between channels
4 - Wider division between channels at center of board
5 - Guide rule
6 - Groove in which guide rule slides
7 - Wooden strip (Guide-rule stop)
8 - Numbering strip

Cipher Device M-138-A (Wood) has always been called by its short title; SIGWOO, even in official instructional documents. SIGWOO is a flat wooden board (13" x 15"), the operating surface of which is equipped with thirty grooved channels (1). These channels are designed to hold changeable paper strips containing random-mixed alphabets. The horizontal divisions (3) between the channels are a little less than 3/16" wide, with the exception of the middle division (4) which is 9/16" wide.

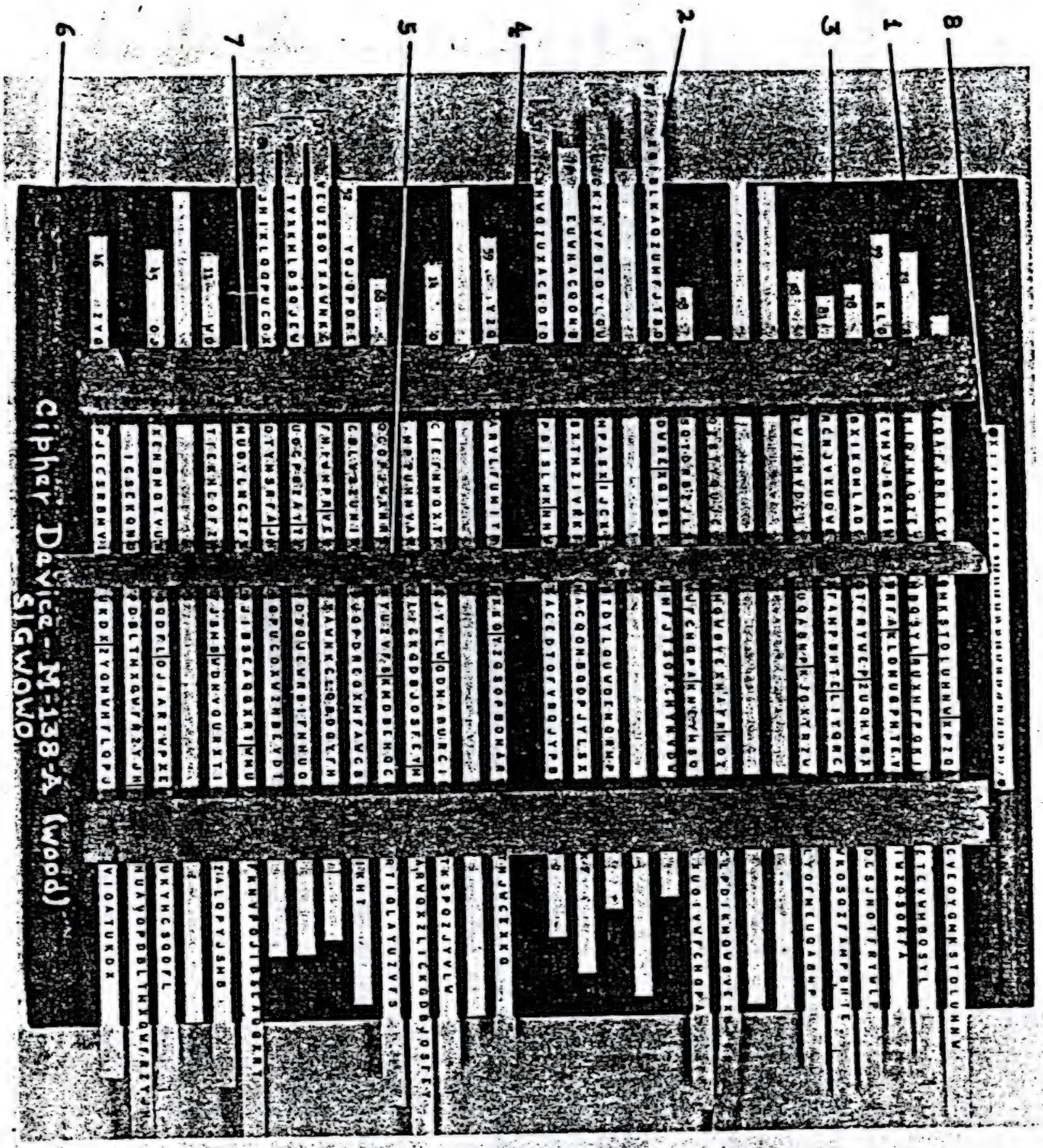
At the bottom of the channeled board is a groove (6) $\frac{1}{2}$ in. wide. In this groove is a small rectangular wooden block to which a wooden guide rule (5) is attached with small nails. The sliding of this block in the groove allows the operator to position the guide rule at any place beneath two strips of wood (7), 1 in. wide, which are nailed to the board in a vertical position and which act as stops for the guide rule. The thirty channels are numbered on the wooden strip at the left.

The space between the wooden strips is such that when the guide rule is pushed to the extreme left and the letters on the alphabet strips are aligned in a vertical column, 27 columns of letters are visible between the guide rule and the right wooden strip. At the top of the board is a series of numbers (8) from 1-25, preceded and followed by the letter "X". These numbers are so positioned that when alphabet strips are inserted in the channels and a column of letters is aligned under either "X", the resultant 25 columns of letters are correctly numbered.[1]

---

1. The method of operation is explained on the page following this photograph.

SECRET


6
7
5
4
2
3
1
8
Cipher Device - M-138-A (Wood)
SIGWOD

~~SECRET~~

METHOD OF OPERATION

The method of operation is as follows: To encipher, first push the guide rule to the extreme left. Then align, in turn, the plain-text letters of the message in a column under either "X", whichever is nearer to the letter being aligned on the particular strip concerned. Starting with the first strip, place the eraser of a lead pencil on the strip directly over the letter to be aligned and push the strip to the left until the pencil is stopped by the guide rule or to the right until stopped by the right wooden strip. Continue this procedure until a complete column of letters has been aligned. Choose a cipher-text column at random by sliding the guide rule and placing it adjacent to any one of the numbers, 1-25, at the top of the board; this is the stage of encipherment pictured on the previous page. Note the plain-text alignment under both "X's".

Copy in 5-letter groups, the cipher-text column thus selected. Repeat the above procedure as many times as necessary to completely encipher the message, provided the message does not exceed the length limit (see page 79), in which case it will be divided into parts. To decipher, align the cipher-text letters in a column beneath either "X" and find the plain-text column beneath one of the numbers from 1-25.

~~SECRET~~

U. S. Army

APR 7 - 1938

No. 71-716-B
April 7, 1938
Superseding No. 71-716-A
of January 3, 1935.

SPECIFICATION

CIPHER DEVICE M-138-A

A. APPLICABLE SPECIFICATIONS AND DRAWINGS

A-1. The attached annex contains a list of the latest issues of specifications and drawings which form a part of this specification. The annex is revised from time to time and the issues of the annex are numbered consecutively starting with number one. Any references made in this specification to other specifications or drawings are made with the issue letters or numbers omitted.

B. TYPES

B-1. This specification covers one type of equipment designated as Cipher Device M-138-A. This consists of an aluminum alloy alphabet strip holder contained in a fabric case.

C. MATERIAL AND WORKMANSHIP

C-1. All parts shall be manufactured and finished in a thoroughly workmanlike manner and in accordance with the best commercial design and practice. All dimensions, except where individual tolerances are given on the drawings, shall be held as close as is consistent with good shop practice.

C-2. Substitution of Materials. If the bidder desires to substitute another material or fabricated part in those cases where the specification and drawings call for the product of a specific manufacturer "or equal," he shall submit a statement to that effect with his bid describing the proposed substitutions and will submit data that will substantiate his claims that such substitutions are the equal of those specified. At the discretion of the contracting officer, samples may be required which will demonstrate by test the suitability of the proposed substitute.

D. GENERAL REQUIREMENTS

D-1. See Section E.

20

E. DETAIL REQUIREMENTS

E-1. All construction shall be in accordance with the drawings listed in the annex.

F. METHODS OF INSPECTION AND TESTS

F-1. The contractor shall furnish all necessary facilities and equipment for making the tests and inspection required by this specification, and shall carry out all tests under the supervision of the inspector. The inspector shall ascertain that all requirement of this specification have been complied with, and may make such other tests as are necessary to determine full compliance with specification requirements even though such tests are not specifically described herein. The contractor shall correct all faults which are pointed out by the inspector and which are contrary to this specification.

F-2. Each cipher device including carrying case shall be carefully examined by the inspector to ascertain that materials, finish and dimensions are as specified on the drawings.

G. PACKAGING, PACKING AND MARKING

G-1. Packaging. The articles shall be placed in individual cardboard cartons so designed as to provide adequate protection. Each carton shall be marked or labeled with name and type of article, order number, date of order and name of contractor.

G-2. Packing. Consignments shall be prepared for either domestic or export shipment as specified by the contracting officer at the contractor's expense in such a manner that they will reach destination in a satisfactory condition.

G-3. Marking. Shipments shall be marked in accordance with U.S. Army specification No. 100-2.

H. NOTES

H-1. The use of this specification, whenever applicable, is mandatory on all procuring agencies of the Army.

H-2. Notice. When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely related Government procurement operation, the United States Government thereby incurs no responsibility or any obligation whatsoever; and the

fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

H-3. Copies of this specification may be obtained from the office of the Chief Signal Officer, War Department, Washington, D.C.

No. 71-71c-B
April 17, 1938
Amendment No. 1

CIPHER DEVICE M-138-A

1. Section D. Delete and replace by the following as Section D:

"D-1. Preproduction Sample. Subject to the provisions of the circular proposal and contract, the following requirements for samples shall apply:

"D-1a. After award of contract, the contractor shall submit two samples of Cipher Device M-138-A for approval. One sample shall be destroyed in test and the other shall be returned to the contractor, if approved, and will be used by the inspector as a standard of workmanship.

"D-1b. If the samples are disapproved, the contractor may be required to furnish additional samples until two satisfactory samples have been submitted. Such additional samples shall be accompanied by a description of the changes which have been incorporated in the new samples in order to correct the faults of the preceding ones. Approval of the submitted samples shall not be construed as authorizing any deviation from the requirements of this specification.

"D-1c. Liability. Any damage to submitted samples resulting from testing or from assembling or disassembling shall be at the contractor's risk. All transportation charges involved in submitting samples for approval shall be at the contractor's expense."

2. Section E. Delete and replace by the following as Section E:

"E-1. General. All construction shall be in accordance with the drawings in the annex except that where drawing notes call for aluminum alloys 52S-H and 53S-E, an equivalent secondary aluminum alloy, or aluminum alloy 3-S, or a suitable plastic compound shall be substituted, preference being in the order named. If aluminum alloy is used, it shall provide the necessary strength and rigidity for the particular application in which it is used. Alloys containing magnesium or requiring heat treatment are particularly to be avoided. All construction shall be such as to meet the production tests given in section F.

"E-1a. Note. If a plastic compound is used the manufacturer shall be permitted, subject to the approval of the contracting officer, to make such alterations in the cross-section of the plates of the Cipher Device M-138-A as will facilitate the molding operation without materially reducing the mechanical strength of the completed device or altering the basic design. The hinge parts may be molded integral with the halves of the device rather than being fastened with screws as shown on the drawings. A plastic molding compound shall be selected which will provide adequate mechanical strength and which will be capable of meeting the warping test of paragraph F-3.

3. Section F. Add the following paragraphs:

"F-3. Warping Test. If a material other than an aluminum alloy is used, the preproduction sample as well as random samples from each day's factory production shall be subjected to a 90 per cent humidity test at a temperature of 130 degrees Fahrenheit for six hours. Not less than three sample units per 1000 units of production shall be subjected to the test. At the end of this test the bow in the plate, as determined by measuring the distance from a straight edge to the lowest point on the plate, when the straight edge rests on the two highest points of the plate, shall be not greater than 1/8-inch. If more than one third of the samples tested fail to pass this test, the entire day's production and all subsequent production shall be rejected until corrective measures have been taken."

4. Paragraph G-1. Packaging. Delete second sentence and substitute the following:

"Each carton shall be marked or labelled with quantity, name and type of article, serial number, order number (usually given on the contract as file number), and name and address of the contractor."

5. Paragraph G-2. Packing. Add at end of paragraph:

"Consignments specified for domestic shipment shall be packed in such a manner as to be capable of being safely reshipped from their original destination to any point within the continental limits of the United States without repacking or reinforcing."

6. Paragraph H-3. Add at end of paragraph:

"However, copies of specifications to be used for the purpose of bidding or manufacture shall be obtained from the contracting officer direct or through an intermediary prospective bidder or contractor."

10-21-40

U. S. ARMY

October 25, 1940.

SPECIFICATION

ANNEX ISSUE NO. 7

TO SPECIFICATION NO. 71-716

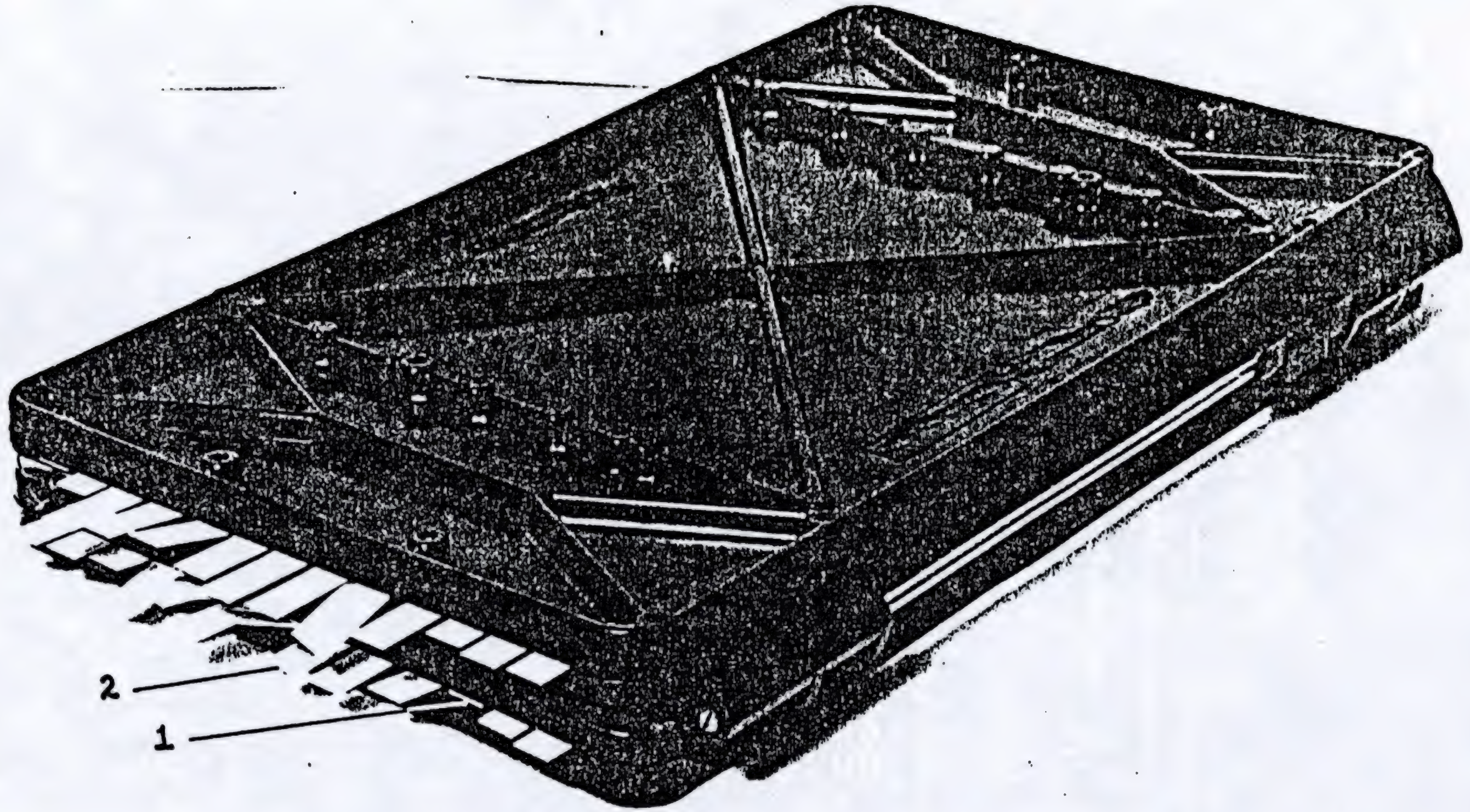
# Denotes change from previous issue.

1. The U. S. Army specification listed below forms a part of this specification:

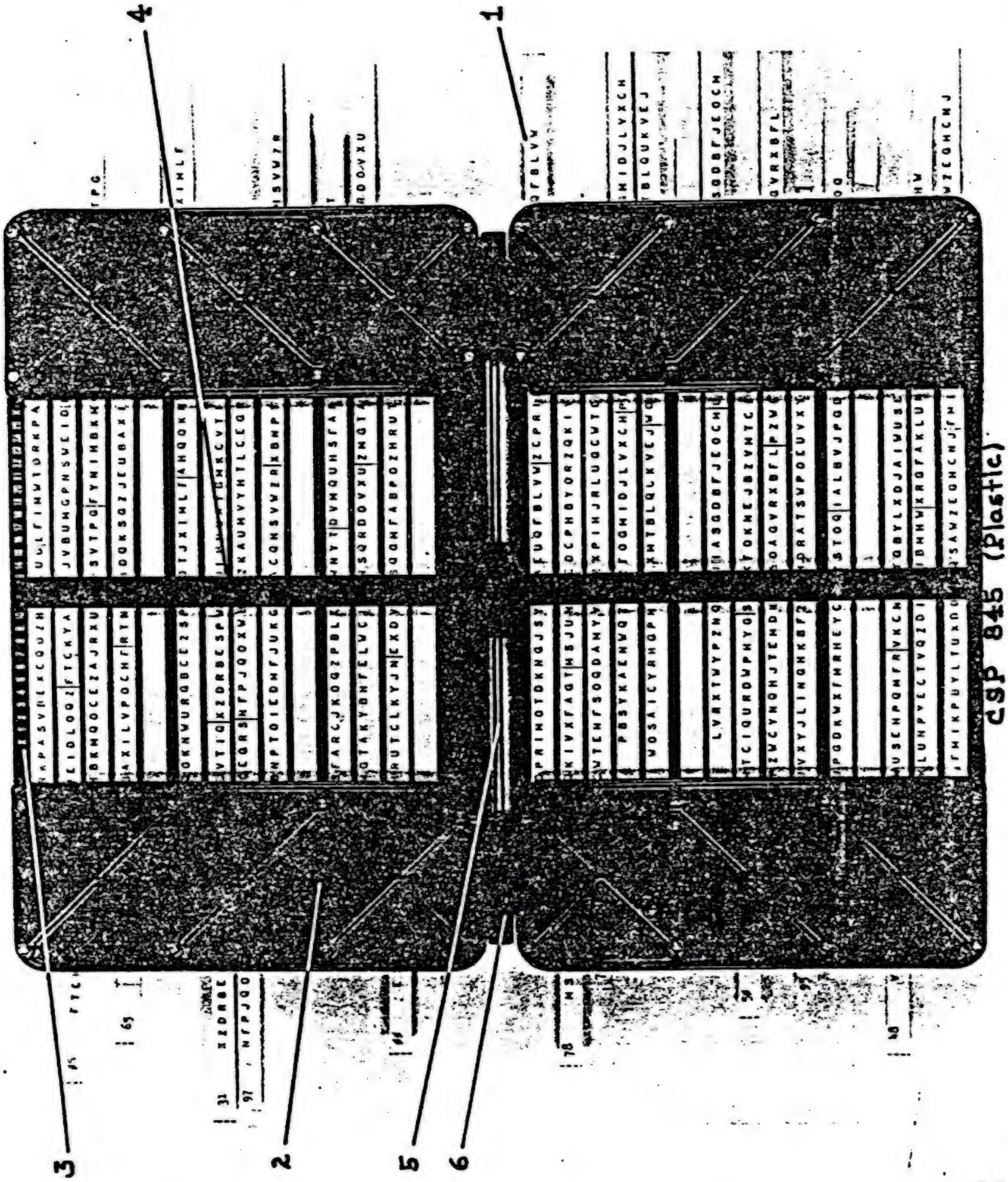
100-2D Standard Specification for Marking Shipments. (Subsidiary specifications not required.)

2. The drawings listed below form a part of this specification:

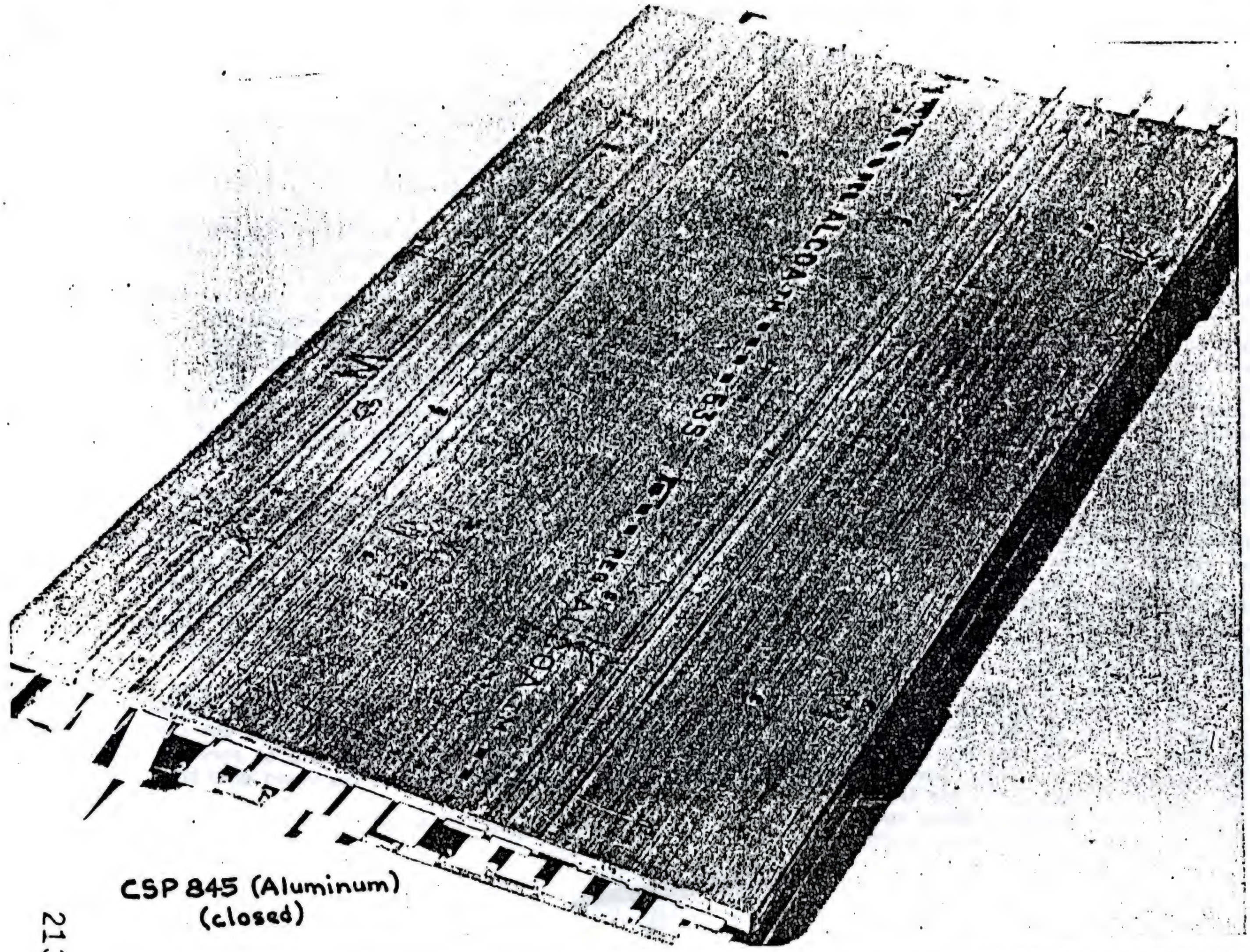
SC-D-1603-B	Cipher Device M-138-A, Assembly
# SC-D-1604-D	Cipher Device M-138-A, Details
SC-D-1605-B	Cipher Device M-138-A, Details
SC-D-2630-D	Cipher Device M-138-A, Carrying Case, Assembly, and Details



CSP 845 (Plastic)
(closed)



CSP 845 (Plastic)



CSP 845 (Aluminum)
(closed)

[redacted]

DETAILED DESCRIPTION OF CIPHER DEVICE CSP 845 (ALBERTUS)

Photograph Opposite

1 - Channel
2 - Alphabet strip
3 - Horizontal divisions between channels
4 - Aluminum strips
5 - Small metal square
6 - Numbering strip
7 - Hinge allowing board to fold
8 - Hinged guide rule
9 - Slender cylindrical rod
10 - Groove in which guide rule slides

Cipher Device CSP 845 is a hinged aluminum board (14" x 12") into which are milled thirty grooved channels (1) (5/16" wide). These channels are designed to hold changeable paper strips (2) containing random mixed alphabets. The horizontal divisions (3) between the channels are 1/8" wide.

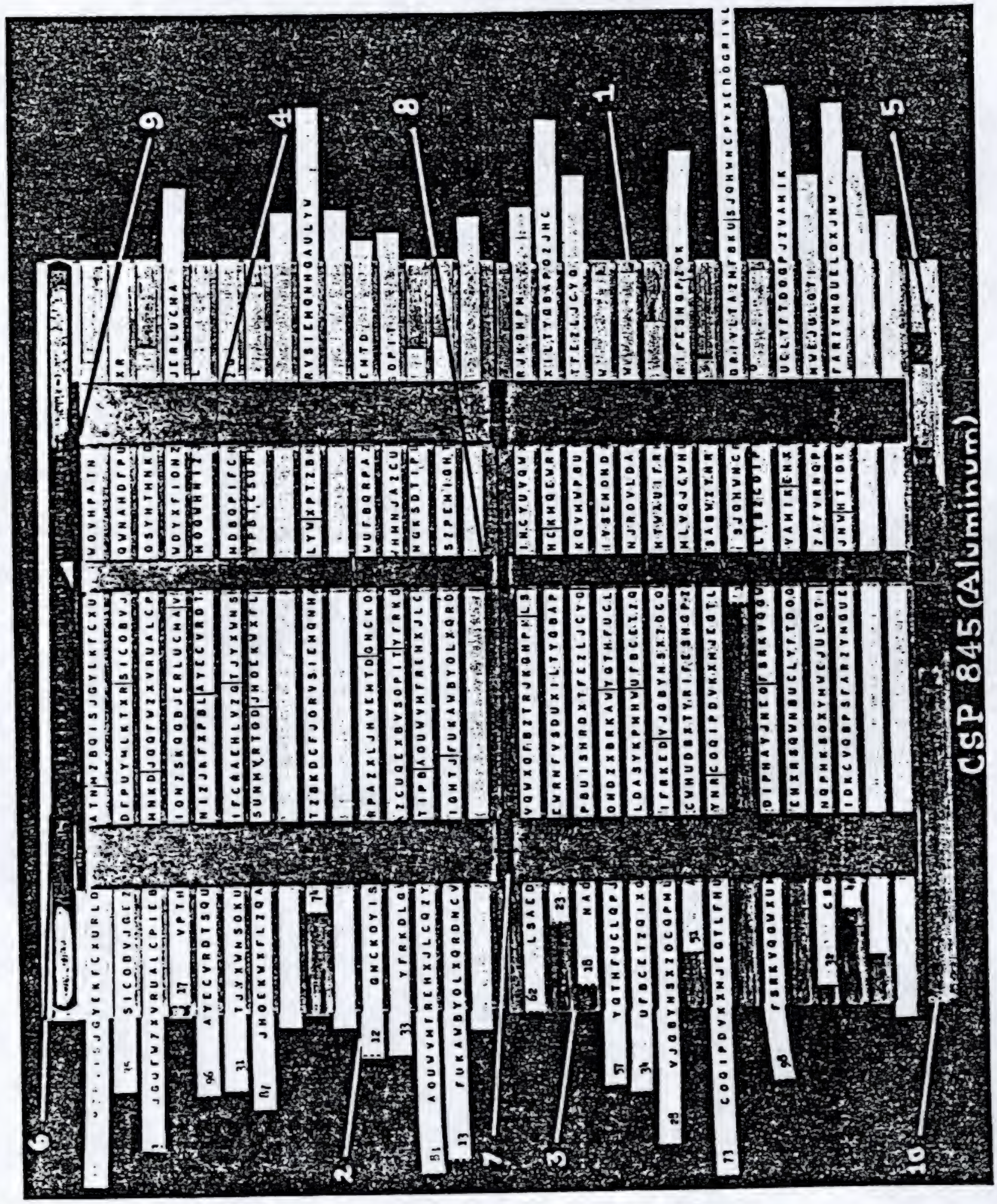
At the bottom of the channeled board is a groove (10), 3/8" wide. In this groove is a small metal slide to which a guide rule (8) is riveted. Two aluminum strips (4), 1" wide, are attached to the board in a vertical position approximately 2 in. from the edges of the board. The aluminum strips are attached to the board by rivets at about every fifth division between the channels. The left aluminum strip acts as a stop for the guide rule. However, the guide rule is prevented from ever touching the right aluminum strip by a small metal square (5) which is riveted in the groove at the bottom of the board. If the guide rule is pushed to the extreme right and is thus stopped by this small metal square, one column of letters aligned on the alphabet strips is visible to the right of the guide rule.

The space between the aluminum strips is such that, when the guide rule is pushed to the extreme left and the letters on the alphabet strips are aligned in a vertical column, 27 columns of letters are visible between the guide rule and the right aluminum strip. At the top of the board is a series of numbers from 1 to 25, preceded and followed by the letter "X". These numbers are so positioned that when alphabet strips are inserted in the channels and a column of letters is aligned under either "X", the resultant 25 columns of letters are correctly numbered. In front of the number series (6) at the top of the board is the designation "CSP 845". (When the board was first issued, it was classified CONFIDENTIAL and was so marked. However, this inscription was deleted when the classification was removed from the board in November 1944.) (See page 61)

The channeled board is made in two sections connected by hinges (7). These hinges are located in the center of and are part of the aluminum strips. The guide rule (8) is also hinged, thus allowing the operator to fold the board. A slender cylindrical rod (9) crosses the space between the two aluminum strips at a point just above the channels. This small rod is attached by means of screws. The purpose of this small rod is to keep the top half of the guide rule close to the board when the top half of the board is being opened or closed.

The method of operation is identical to that of the plastic device (Tab 30).

[redacted]


CSP 845 (Aluminum)

[redacted]

DATE	NUMBER OF DEVICES PROCURED: M-138	M-138-A	CSP 845 (Plastic)	CSP 845 (Metal)	SIGWOWO	ORDER NO. AND PROCUREMENT AUTHORITY	COST	CUMULATIVE TOTALS
7 Jan. 1935	30					Order No. SC-103555, R. No. 2056. Authority: SC-5367-P-1-3059-A-545-56	$450.00	
20 Aug. 1935	60					Order No. SC-103607, R. No. 3717. Authority: SC-6368-P-1-3059-A-545-56	900.00	
26 Nov. 1935	60					Order No. SC-103622, R. No. 3717. Authority: SC 6368-P-1-3059-A-545-56	900.00	150 M-138
1939		224[1]				Exact date of procurement and Order No. unknown	3,360.00[4]	
27 Sep. 1940		550				Order No. 1070-NY-41, DP 41-155	8,250.00	
Later 1940		60				Order No. 1070-NY-41, DP 41-804	900.00[4]	
Jan. 1941		120				Order No. 3338-NY-41, DP 41-1139	1,800.00	
Fall 1941		518[2]				Order No. 6011-NY-41, DPs 41-3288 and 41-3202 (Not confirmed as completed)	7,770.00[4]	1472 M-138-A
9 Feb. 1942			1200			Order No. 132-OCSigO-42 Authority: SC 801-P-5-30-A-0605-12	10,200.00[3]	
Fall 1942					50	Order No. unknown (Purchased for experimental purposes)	350.00[4]	
23 Feb. 1943					2000	Order No. unknown	14,000.00	2050 SIGWOWO
9 Dec. 1942			5000			Order No. 496-OCSigO-43 Authority: SC-3247-P-120-09-A-0605-23	45,000.00	6200 CSP 845 (Plastic)
Sep. 1943				8000		Order No. unknown. Purchase Request No. 44-682. Authority: P-120-09 SSA 42-44	80,000.00	8000 CSP 845 (Metal)
						Approximate Totals	$173,880.00	17,872

1. Approximate. The number is based upon Distribution List (Tab 36).
2. See text page 51.
3. Correspondence gives this figure as an estimated cost.
4. Figures are estimated by using same rates as those given on other contracts. Unchanging rates are assumed to be accurate because the contracts available demonstrate that the rates did not change according to the quantity ordered.

The records of Army Security Agency concerning the costs of these devices are not complete, because such records during the specified periods were not entirely under the control of this Agency or its predecessors. If more accurate figures are required it is suggested that the information be secured from the Philadelphia Signal Corps Procurement District, Philadelphia, Pennsylvania.

[redacted]

CHRONOLOGICAL OUTLINE OF PROCUREMENT OF STRIP CIPHER DEVICES

Date	M-138-A	CSP 845 (Plastic	SIGWOWO	CSP 845 (Metal)
Jan '42	Widdin Metal Goods Co. had delivered 254 by this date. 518 more due in April bringing the total delivered to 1,472.			
22 Jan '42		Purchase request (from SIS to Procurement) for 1200 plastic CSP 845 to supplement supply of M-138-A.		
30 Mar 42	Request for 4,373 M-138-As sent to Phila. Signal Corps Procurement District			
Apr '42	Bid by Widdin on above order recommended use of plastic material because their request for allocation of aluminum had been disallowed by the War Production Board.			

Date	M-138-A	CSP 845 (Plastic)	SIGWOWO	CSP 845 (Metal)
1 Jun 42	SCTC reclassified M-138-A from standard to limited standard.			
22 Oct '42		5000 Navy devices, namely, plastic strip boards, CSP 845, requested by Signal Security Branch from Procurement Division.		
9 Dec '42		Purchase order for the above requested 5000 plastic devices. Cost $45,000.00.		
Jan '43			Inception of SIGWOWO test of 50 at Arlington Hall Message Center.	
Feb '43			Purchase of 2000 wooden devices (SIGWOWO)	
Apr, May '43		Complaints from field on unserviceability of plastic devices. Complaints continued into 1944.		

Date	M-138-A	CSP 845 (Plastic)	SIGWOWO	CSP 845 (Metal)
19 Jul '43		Steps begun to remove CSP 845 (plastic). Ltr sent to continental U.S. holders to return all metal boards.		
Aug, Sep '43			Complaints from field on SIGWOWO	
Sep '43				Aluminum again available - 8000 aluminum devices ordered from - Navy CSP (845).
13 Oct '44				Delivery of 8000 CSP 845 (metal) completed.
20 Dec '44	Ltr. No. 532 from SSB states that CSP 845 (Plastic), SIGWOWO, M-138, and M-138-A have been declared obsolete.			
Early 1945	Completion of reclamation of CSP 845 (Plastic), SIGWOWO, M-138, and M-138-A. Completion of distribution of CSP 845 (Metal).			

~~CONFIDENTIAL~~

WAR DEPARTMENT
ARMY SERVICE FORCES

TRANSMITTAL SHEET

Office of the Chief Signal Officer Action 1 SPSIC-2

THRU			
TO	Chief, Army Communications Service (Service, division, or organization)		Room 4E 250, The Pentagon (Location)
	Chief Signal Officer (Branch or unit)		Room 3E 200, The Pentagon (Attention)
Subject:	Removal of Classification and Registry and Exemption from Property Accountability of Cipher Device CSP 845 and Similar Devices		
File No.	SPSIC 461 Codes	Chittenden (Writer's last name)	16 November 1944 (Date)
FROM	Signal Security Branch (Service, division, or organization)	Room 3C 340 (Location)	Code 8129, Ext 269 (Telephone extension)

1. It is requested that authority be obtained from the Commanding General, Army Service Forces to exempt the CSP 845 and all other strip cipher devices from property accountability upon removal of the present classification and registry, and that the Signal Security Agency be charged with the storage and issue of the devices if this authority is obtained.

2. At the present time the CSP 845, a Navy device purchased by the Army, and other similar Signal Corps devices (SIGWOWO and SIGOUDJ) are confidential, registered cryptographic devices and are stored, issued, and accounted for by the Signal Security Agency in accordance with the provisions of AR 380-5. They are issued by the Signal Security Agency only to authorized holders of United States Army cryptographic systems. Obsolescent devices, M-138 and M-138-A, are classed as items of property and are being withdrawn from use as rapidly as possible in order to standardize the strip cipher devices in use in the field.

3. A serious accounting problem has been encountered due to the removal of the classification and registry from the CSP 845 by the Navy Department and their handling it as an unclassified item for which no accountability is required. This action was effected by a memorandum, 21 September 1943, issued by the Director of Naval Communications, which is quoted as follows:

"CSP 845, Strip Cipher Device, is no longer a classified device. Obliterate the word "CONFIDENTIAL" and the register number from all copies, and remove from routine accountability. This device will continue, however, to bear the short title CSP 845 and to be issued through the Registered Publications Section."

4. Many Army holders of cryptographic material became aware of this memorandum, assumed that it applied to all CSP 845's, and ceased accounting for all in their possession.

5. The problem grows more complex daily because Overseas Naval Issuing Offices will and do issue unclassified, unregistered CSP 845's to Army units upon request. This results in the Army units' holding some devices for which they must account as registered, classified devices and some for which no such accounting is required. The resulting confusion is causing unnecessary correspondence and waste of time.

220

W. D., A. G. O. Form No. 0105
March 27, 1943.

24-70991

~~CONFIDENTIAL~~

6. The need for registry and classification of strip cipher devices issued by the Chief Signal Officer no longer exists. However, it is essential that they continue to be stored and issued by the Signal Security Agency, which also stores and issues the other integral cryptographic materials necessary for operating the system. It is also necessary that the devices be issued through cryptographic channels, which differ greatly from property channels.

7. CSP 845, SIGWOWO, and SIGOUDJ are not now items of Tables of Organization and Equipment and are exempt, by the provisions of paragraph 38d, AR 380-5, 15 March 1944, from property accountability under the general provisions of AR 35-6520. Since this exemption would cease upon removal of classification and registry, it is necessary, in order that storage and issue of these devices be continued by the Signal Security Agency, to secure their re-exemption from property accountability. Exemption of the obsolescent devices, M-138 and M-138-A, from property accountability is desired to afford uniform handling of all strip cipher devices.

8. The requested exemption may be accomplished under the provisions of paragraph 3c, AR 35-6520, quoted below:

"The Commanding General, Services of Supply, may authorize chiefs of supply to exempt from property accountability designated items of supply in designated units, agencies, or organizations. With the approval of the Commanding General, Services of Supply, chiefs of supply will issue instructions which are consistent with keeping an adequate record of such designated items of supply."

9. Upon removal of classification and registry and exemption from general property accountability, the devices will continue to be accountable to the Chief Signal Officer, in a manner similar to that prescribed for registered, classified cryptographic materials, as described in Inclosure 1.

10. A memorandum for the Commanding General, Army Service Forces, implementing this request, is forwarded for signature.

W. Preston Corderman

W. Preston Corderman
Colonel, Signal Corps
Chief, Signal Security Branch
SPSIS-1, Code 8129, Ext 211

2 Incls.
Incl 1. Copy of proposed letter to all holders of CSP 845, SIGWOWO, and SIGOUDJ
Incl 2. Memo for CG, ASF, file as above, subj "Exemption of Cipher Device CSP 845 and Similar Devices from Property Accountability," with 1 Incl

ARMY SERVICE FORCES

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON 25, D. C.

SPSIC-2
Letter No. 531

20 December 1944

Subject: Removal of Classification and Registry and Subsequent Responsibility for Cipher Devices CSP 845, SIGWOWO, and SIGOUDJ

To: All holders of the Subject Cipher Devices

1. Classification and registry of cipher devices CSP 845, SIGWOWO, and SIGOUDJ have been removed. They will continue to bear their present respective short titles, but the word CONFIDENTIAL and the register number should be obliterated from all copies.

2. Accountability will continue to the Chief Signal Officer, through cryptographic channels, as prescribed below.

a. Accounting will be similar to that prescribed for registered, classified cryptographic materials, except that report by register number will not be made. Only the total number of these devices, indicated by short title, will be shown on reports of possession, transfer, or destruction.

b. WD Form 34, WD Form 34a, or WDSC Form 86 will be used for reports on these devices.

c. Damaged or unserviceable devices, which cannot be repaired, will be returned to the Chief Signal Officer for salvage.

3. All holders are responsible for the care and safekeeping of these devices and for their ultimate return to the Chief Signal Officer when they are no longer required.

For the Chief Signal Officer:

Frank E. Stoner
Major General, U. S. Army
Chief, Army Communications Service

S. P. Collins
Colonel, Signal Corps
Acting Chief, Signal Security Branch

FOR VICTORY BUY WAR BONDS AND STAMPS

HEADQUARTERS, ARMY SERVICE FORCES

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON 25, D. C.

SPSIC 461 Codes

SPSIC-2

18 November 1944.

MEMORANDUM for Commanding General, Army Service Forces

Attention: Director of Supply

Subject: Exemption of Cipher Device CSP 845 and Similar Devices from Property Accountability

1. It is requested that authority be granted, under the provisions of paragraph 3c, AR 35-6520, to exempt Cipher Device CSP 845 and all other strip cipher devices from property accountability, and that the Signal Security Agency be charged with the storage and issue of these devices.

2. Exemption from property accountability of Cipher Device CSP 845 and all other strip cipher devices (SIGWOWO, SIGOUDJ, M-138, and M-138-A) is necessary for the following reasons:

a. At the present time CSP 845, SIGWOWO, and SIGOUDJ are confidential, registered components of several cryptographic systems and are stored, issued, and accounted for by the Signal Security Agency.

b. The Signal Security Agency proposes to remove classification and registry from these devices, since the United States Navy has already done so. Upon removal of classification and registry, the existing exemption from property accountability under the general provisions of AR 35-6520, as cited in paragraph 38d, AR 380-5, 15 March 1944, will cease.

c. Obsolescent devices, M-138 and M-138-A, are presently classed as items of property. However, they are being withdrawn from use as rapidly as possible in order to standardize the strip cipher devices used in the field. Their exemption from property accountability is desired to afford uniform handling of all such devices.

d. It is essential that these devices continue to be stored and issued by the Signal Security Agency, which also stores and issues the other integral cryptographic materials necessary for operating the systems. It is also necessary that they be issued through cryptographic channels, which differ greatly from property channels.

[redacted]

EO-6955-1C

SPSIC 461 Codes SPSIC-2

3. Upon exemption from general property accountability, these devices will, in compliance with the requirements of paragraph 4, AR 35-6520, be accounted for in the manner prescribed in the accompanying inclosure.

For the Chief Signal Officer:

James A. Code, Jr.,
Major General, U. S. Army,
Assistant Chief Signal Officer.

1 Incl.
Copy of proposed letter to all holders of CSP 845, SIGWOWO, and SIGOUDJ

SPDDI 475.7
Serial No. 36440

1st Ind.

NOV 23 1944

Headquarters, Army Service Forces, Washington 25, D. C.
To: The Chief Signal Officer:

1. Request contained in paragraph one (1) of basic communication is approved.

By command of Lieutenant General SOMERVELL:

F. A. HEILEMAN,
Brigadier General, G.S.C.,
Director of Supply, A.S.F.

1 Incl:
n/c

DON B. KATES,
Lt. Colonel, General Staff Corps,
Executive, Operations Branch,
Distribution Division, A.S.F.

[redacted]

30 224

SECRET

DISTRIBUTION AND NUMBER AUTHORIZED ON HAND OF CIPHER DEVICES M-138 and M-138-A

SEPTEMBER 9, 1939

	M-138 Auth. on Hand	M-138-A Auth. on Hand
War Dept. (Message Center)	[illegible]	[illegible]
Corps Areas	18	1[illegible]
Overseas Departments	42	[illegible]
General Headquarters		
Ports of Embarkation		2
Expeditionary Forces		
Coastal Frontiers	4	
Sectors, Coastal Frontiers	1[illegible]	
Subsectors, Coastal F.	1[illegible]	
C. A. Districts	[illegible]	[illegible]
Harbor Defenses	2[illegible] (c)	[illegible]
Army Transports		[illegible]
Mine Planters		[illegible]
Groups of Field Armies		
Field Armies		
Army Corps		
Divisions		
Brigades		
Regiments		
Battalions		
GHQ Air Force	[illegible]	[illegible]
Wings GHQ Air Force	1[illegible]	[illegible]
Air Corps Task Forces	(b)	
[illegible]	[illegible]	
[illegible]		
[illegible]		
[illegible] Navy Liaison Officer		
Military Attachés in Europe		
" " Americas		
" " Far East		
[illegible], Depots, Arsenals	[illegible]	1[illegible]
[illegible] Pacific Sectors	[illegible]	[illegible]
Governor General of Philippines	[illegible]	
Panama Canal		[illegible]
[illegible]		
[illegible] Total	[illegible]	[illegible]
Total	[illegible]	[illegible]

(a) Includes 5 Overseas Departments.
(b) [illegible] to 19th Wing.
(c) [illegible] including 2 [illegible] of San Juan.
(d) [illegible]
(e) [illegible]
[illegible]

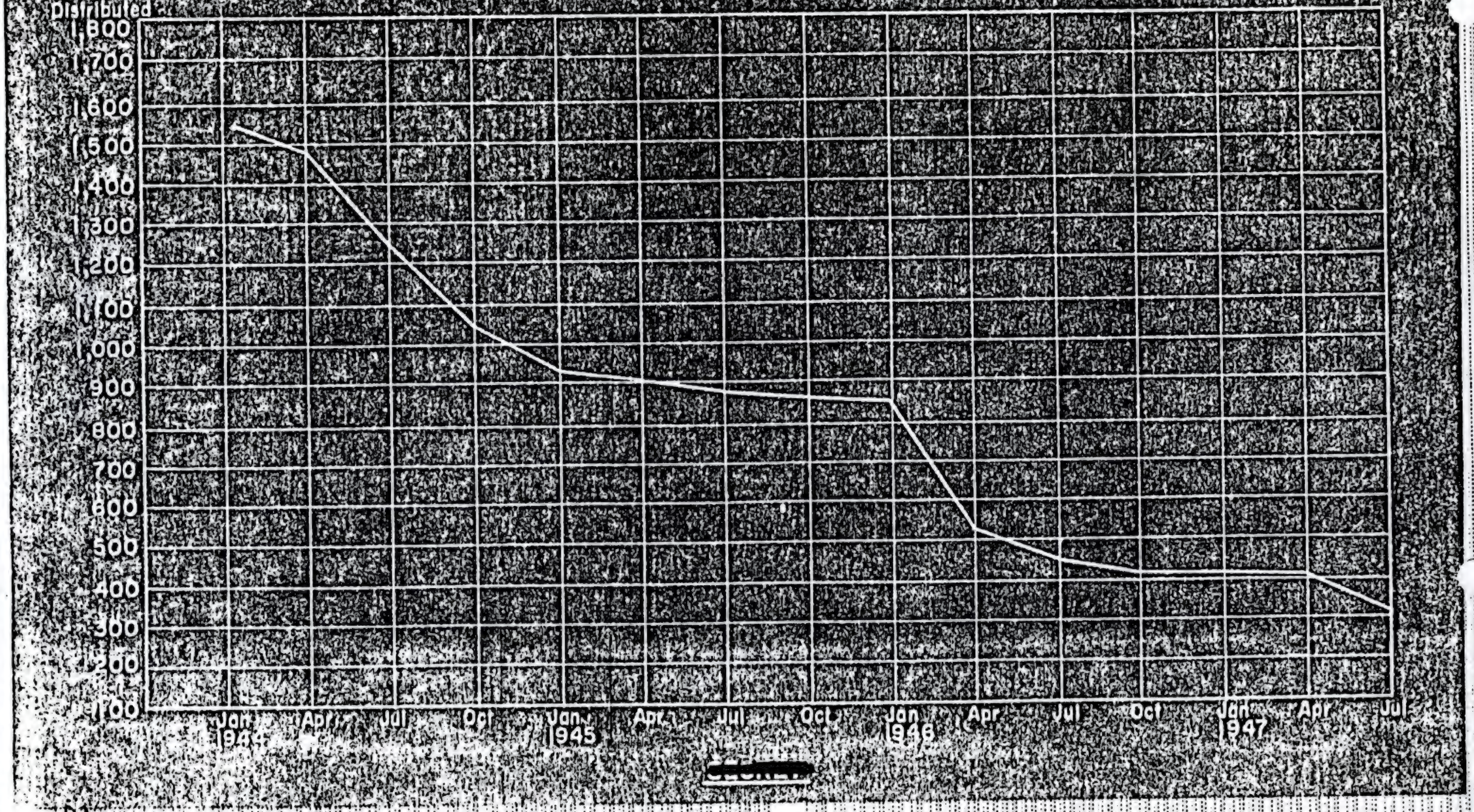
[illegible] Filler Cipher Device M-138.

SECRET

SECRET

Distribution of System 150: Feb. 44 - Sep 47

(System 150 was the most widely held strip system.)



SECRET

OUTLINE OF CRYPTONET DISTRIBUTION OF STRIP SYSTEMS DURING WORLD WAR II[1]

The following outline of distribution of strip systems within the cryptonets during World War II is intended to provide enlargement of a general concept. It is a supplement to Chapter VIII and should not be considered as a separate item. Neither should it be used for determination of facts concerning specific status of a strip system for three reasons: First, the information concerning the holders has been generalized; second, effective dates are, in many cases, approximate and sometimes indeterminable; and third, events [illegible] that [illegible] after the writing of this outline may bring changes in the status of a system.

For those readers to whom the concept of the cryptonets is new, the following brief explanation, introductory to the outline, is provided.

Cryptonets are communications networks which isolate similar types of headquarters into different strata of cryptographic communication, and separate the internal cryptographic communications of one theater of operations from those of another. The cryptonets were designed to provide cryptographic communications between headquarters the functions of

---

1. Although many of the notes in this Appendix are carried beyond the end of World War II, the issue of Converter M-228/[illegible] (SIGCUM) has been mentioned but has by no means been carried to completion. At the time of writing ([illegible]), plans for issue of SIGRED or [illegible] replacement for Converter M-134-C ([illegible]) were being effected in many of the cryptonets.

which are similar and which need cryptographic communications to function properly.

The cryptonets are divided generally into four categories, world-wide, area (theater), joint, and special. A world-wide cryptonet consists of those headquarters that require inter-communication irrespective of geographical location. An area (theater) cryptonet is composed of those headquarters located within a specific geographical area. A joint cryptonet consists of Army and Navy headquarters located throughout the world which require inter-communication. Special cryptonets are all other cryptonets which are formed to cover specialized communication requirements such as those of the Army Security Agency, Military Attaches, and Army and Airways Communications System.

The cryptonet basic document lists the holders of the various cryptosystems which make up the cryptonet. These systems are separated generally into three categories for use, very high command, high command, and general. Each succeeding higher command in the net uses separate cryptosystems within its own echelon and holds in addition to its own cryptosystems, the cryptosystems held by the lower echelon.

Specifically, distribution of strip systems in the cryptonets was as follows:

1. Cryptonet AB. (General world-wide; most widely distributed of all cryptonets)

a. Normal Strip systems.

(1) System No. 1501

(a) Common normal world-wide system for those holders authorized alphabet strips but not SIGABA.

(b) Effective: 22 February 1944 - [1]

(c) Distribution: Through all levels of command from War Department and high command headquarters down to and including posts, camps, and stations.

(d) Discussion: After World War II, on 15 March 1946, Cryptonet 15 superseded Cryptonets 12, 13, and 14. Systems 1501 and 1502 continued as previously. See 1b(3) for System No. 1501 as stand-by system.

(2) System No. 1502.

(a) Common normal strip system for holders in Continental U. S. only, authorized alphabet strips but not SIGABA.

(b) Effective: Early 1944 - 1 December 1946.

(c) Distribution: Only within Continental limits of U.S. through all levels of command from War Department and high command headquarters down to and including posts, camps, and stations.

(d) Discussion: This system cut down traffic load in strip System No. 1501 by providing a seperate strip system for Continental U. S. holders.

---

1 In follow-up date after the dash means that the system was still effective at the time of writing: August 1947.

Providing systems called "Continental Group" was a policy in two of the general world-wide cryptonets, 15 and 14. Domestic System No. 1502 was discontinued 1 December 1946 after which time traffic formerly handled in this system was enciphered in System 1501.

b. Stand-by Strip Systems.

(1) System No. 1521.

(a) Common stand-by strip system.

(b) Effective: September 1943 -

(c) Distribution: Through all levels of command from War Department and high command headquarters down to and including posts, camps, and stations. Included both overseas and U. S. holders.

(d) Discussion: System 1521 has always been a stand-by strip system for System 1501 except during the first few months of its issue when it was a normal system. After World War II, beginning in March 1946, it acted as stand-by system for both normal System 1501 and normal System No. 1502.

(2) System No. 1522.

(a) Common stand-by system for holders, in Continental U. S. only, authorized alphabet strips but not rotors (that is, stand-by for System No. 1502).

(b) Effective: 16 September 1943 - March 1946

(c) Distribution: Only within Continental limits of U. S. through all levels of command from War Department and high command headquarters down to and including posts, camps, and stations.

(d) Discussion: System No. 1522 was always a stand-by strip system except during the first few months of its issue when it was a normal system. After World War II, in March 1946, it was superseded by stand-by strip System No. 1521

(3) Systems No. 1501 and 1502. - Discussion: On 15 March 1946, Systems No. 1501 and 1502 became stand-by systems for the two new systems of Cryptonet 15 which were established as replacement systems for Cryptonet 14.[2] System No. 1501 became stand-by for the world-wide SIGABA System No. 1503[2] and System No. 1502 became stand-by for the domestic SIGABA System No. 1504.[2] On 1 December 1946, when System No. 1501 was discontinued, System No. 1501 became stand-by for System No. 1504 as well as System No. 1503. After Systems No. 1501 and 1502 became stand-by systems, they served in dual capacity since they retained their status as normal systems for holders authorized alphabet strips but not SIGABA. See also Systems No. 1501 and 1502 under Normal Systems above.

4. Cryptonet 14. (General world-wide; Army through Divisions)

a. Normal Strip Systems. - None.

b. Stand-by Strip Systems.

(1) System No. 1421.

(a) Common stand-by strip system for normal SIGABA System No. 1401.

(b) Effective: 7 September 1943[3] - 15 March 1946

(c) Distribution: Through all levels of command from War Department and high command headquarters down to and including Divisions. Included both U.S. and overseas holders.

(d) Discussion: Discontinued when Cryptonet 14 was superseded by Systems No. 1501 and 1504.

---

2. System No. 1503 replaced Cryptonet 12; System No. 1504 replaced Cryptonet 13; and System 1503 (world-wide) replaced Cryptonet 14.

3. [illegible] September 1943, Cryptonet 14 stay used System No. 1421.

(2) System No. 1422

(a) Common stand-by strip system for holders, in Continental U. S. only, authorized alphabet strips but not SIGABA.

(b) Effective: 7 September 1943 - 15 March 1946.

(c) Distribution: Only within Continental U. S. through all channels of command from War Department and high command headquarters down to and including Divisions.

(d) Discussion: Used as stand-by strip systems for normal SIGABA System No. 1402.

f. Cryptonet 13. (General world-wide; down through base commands)

a. Normal Strip System. - None.

b. Stand-by Strip System.

(1) System No. 1521.

(a) Common stand-by strip system for normal SIGABA System No. 1311.

(b) Effective: 15 August 1943 - February 1945.

(c) Distribution: Through all levels of command from War Department and high command headquarters down to and including base commands.

(d) Discussion: Discontinued in February 1945 because of new policy explained in footnote 4 below.

---

* Ltr, No. 540, SPSIC-2, TO: All Holders of Cryptonet 12 and Cryptonet 13. Signed: For the Chief Signal Officer: By Maj. Gen. Irwin D. Chaney, U. S. Army, Chief, Army Communications Service and Lt. Colonel E. Hyde, Signal Corps., Signal Security Branch, Subject: Discontinuance and Destruction of Stand-by Alphabet Strip System in Cryptonet 12 and 13; dated 12 February 1945.

"1. In accordance with the Chief Signal Officer's

(2) Systems No. 1322, 1323, 1324, 1325, 1326, 1327

(a) Isolation stand-by strip systems for normal strip systems No. 1302, 1303, 1304, 1305, 1306, 1307, respectively.

(b) Effective: 15 August 1943 - May 1944.

(c) Distribution: War Department and one or two holders in field, usually only one. (Isolation systems for communication between holder and WAR. See distribution of System 1321 (page 4) for levels of command included.)

(d) Discussion: Cryptonet 15 obsolete 15 March 1946.

Cryptonet 12. (General world-wide; WAR and Theater Headquarters)

a. Normal Strip Systems. - None.

b. Stand-by Strip Systems.

(1) System No. 1221.

(a) Common stand-by strip system for normal SIGMA System No. 1201.

(b) Effective: 7 August 1943 - February 1944.

---

program of eliminating strip cipher systems which are rarely used and for which a necessity to maintain exists, the stand-by alphabet strip systems in Cryptonets 12 and 15 are being discontinued. The distribution scheme of these two cryptonets now precludes the necessity for individual stand-by systems.

"2. Under the cryptonet plan, all holders of Cryptonet 12 hold Cryptonet 15, and all holders of Cryptonet 15 also hold Cryptonets 14 and 15. If for any reason, a normal system in Cryptonet 12 becomes inoperative, the normal system in Cryptonet 15 may be used. Similarly, if the normal system in Cryptonet 15 is inoperative, the normal system in Cryptonets 14 and 15 can be used."

(c) Distribution: War Department and Theater Headquarters. (Included some base commands.)

(d) Discussion: Discontinued in February 1945 because of new policy explained in footnote 4 on pages four and five.

(2) Systems No. 1222, 1223, 1224, 1225, 1226, 1227, 1228, 1230.

(a) Isolation stand-by strip systems for normal SIGABA Systems No. 1203, 1204, 1205, 1206, 1207, 1208, 1210, respectively.

(b) Effective: 7 August 1943 - February 1945.

(c) Distribution: War Department and one or two holders in field, usually one. (Isolation systems for communication between holder and WAR. See distribution of System 1221 above for levels of command included.)

(d) Discussion: Discontinued in February 1945 because of new policy explained in footnote 4, pages four and five. Cryptonet 12 obsolete 15 March 1946.

(3) Systems No. 1231 and 1232.

(a) Stand-by strip system for normal SIGABA Systems No. 1211 and 1212, respectively.

(b) Effective: 1 April 1944 - February 1945.

(c) Distribution: Distributed to War Department and several departments and high commands.

(d) Discussion: Discontinued according to policy explained in footnote 4, pages four and five.

3. Cryptonet 16. (Military Attache Net) - Superseded by Cryptonet 42 and subsequently by Cryptonets 47, 48, and 49.

a. Normal strip systems.

(1) System No. 1633

(a) Common normal system for military attachés in European Area.

(b) Effective: - 1 May 1946

(c) Distribution: WD, Allied Forces Eq, U.S.M.A.s in Helsinki, Stockholm, Madrid, Lisbon, Tangiers, London, and Gibraltar.[5]

(d) Discussion: All military attachés used strips for normal communication with WAR except U.S.M.A., London, which office holds SIGABA.

(2) System No. 1628

(a) Common normal system for military attachés of Far East.

(b) Effective October 194[illegible] - 1 May 1946.

(c) Distribution: WD, military attachés in Far East Area.[6]

(d) Discussion: Systems 1628, 1629, 1630, 1632, and 1635 were area systems.

(3) Systems No. 1629, 1632.

(a) Common normal systems for military attachés of Latin America.

(b) Effective: October 1943 - 1 May 1946.

(c) Distribution: WD, military attachés in North, Central, and South America. Second basic added: U.S.M.A., Mexico and [illegible] offices. Caribbean Defense Command was added as a holder of only System 1629.[6]

(4) System No. 1630.

(a) Common normal system for military attachés of Near East and Africa.

---

5. When Cryptonet 42 superseded Cryptonet 16 on 1 May 1946, isolation systems (for communication between WAR and the individual M.A.) were added to the M.A. Net. These isolation systems used one-time means of communications, usually one-time pads.

6 Ibid.

(b) Effective: October 1943 - 1 May 1946.

(c) Distribution: WD, Military Attaches in Near East and Africa.

(d) Discussion: Systems 1628, 1629, [illegible], 1632, and 1635.

(5) System No. 1631.

(a) See Distribution.

(b) Effective: October 1943 - 1 May 1946.

(c) Distribution: WD; U.S.A. Forces in Southwest Pacific; Allied Forces HQ.; Asiatic Theater of Operations; Military Attaches in Near East and Africa; Military Attaches in Far East; Middle East Service Commands; Second [illegible] holders: WD: U.S.M.A. in Near East and Africa; U.S.A. Forces in Southwest Pacific; AFHQ Algiers; U.S.A. Forces in Middle East; Asiatic Theater of Operations; Middle East Service Command.

(6) Systems 1622, 1623, 1624, 1625, 1626, 1627, 1633, 1634.

(a) Normal strip systems for limited number of attaches.

(b) Effective: October 1943 (except System 1623 which was effective 1 March [illegible]) - 1 May 1946.

(c) Distribution: All the systems held by WD, U.S.M.A. London and one other Military Attache.

(d) These systems provided, in effect, isolation systems for Helsinki, Stockholm, Madrid, Lisbon, [illegible], Moscow, Gibraltar, and Iceland Base Command, which places were the holders (besides London and WD) of Systems 1622, 1623, 1624, 1625, 1626, 1627, 1633, 1634, respectively.

[illegible] Twenty-[illegible] Items. - None.

Incl.

6. Cryptonet 42. (Military Attache Net). - Superseded Cryptonet 16(1 May 1946) and was itself subsequently superseded by Cryptonets 47, 48, and 49.

c. Normal Strip Systems.

(1) System No. 4201.

(a) Common normal strip system for Military Attaches of European Area.

(b) Effective: 1 May 1946 - 1 August 1947.

(c) Distribution: All military attaches in European Area except U.S.M.A., Moscow and U.S.M.A., Ankara.

(d) Discussion: Superseded by System No. 4901 (see 6a(2)(d) on 1 August 1947 when Cryptonets 47, 48, and 49 superseded Cryptonet 42.

(2) System No. 4203.

(a) Common normal strip system for Military Attaches in European Area with the exception of those in System No. 4201.

(b) Effective: 1 May 1946 - 1 August 1947.

(c) Distribution: To all Military Attaches in European Area except U.S.M.A., Moscow; U.S.M.A., Dublin, U.S.M.A., Stockholm; U.S.M.A., Rome.

(d) Discussion: Obsolete 1 August 1947 when Cryptonets 47, 48, and 49 superseded Cryptonet 42.

(3) System No. 4204.

(a) Common normal strip system of Military Attaches in Far East Area.

(b) Effective: 1 May 1946 - 1 August 1947.

(c) Distribution: All Military Attaches in Far East Area.

(d) Discussion: Superseded by System No. 4904 (see 7a(2) on 1 August 1947 when Cryptonets 47, 48, and 49 superseded Cryptonet 42.

(4) System No. 4221.

(a) Common normal strip system of Military Attaches in Africa-Middle East Area.

(b) Effective: 1 May 1946 - 1 August 1947.

(c) Distribution: All Military Attaches in Africa-Middle East Area.

(d) Discussion: Discontinued 1 August 1947 when Cryptonets 47, 48, and 49 superseded Cryptonet 42.

(5) System No. 4262.

(a) Common normal strip system of Military Attaches in North and Latin American Area.

(b) Effective: 1 May 1946 - 1 August 1947.

(c) Distribution: All Military Attaches in North and Latin American Area.

(d) Discussion: Superseded by System No. 4701 (see 7 below) on 1 August 1947 when Cryptonets 47, 48, and 49 superseded Cryptonet 42.

7. Cryptonets 47, 48, and 49. (Military Attache Net). - The three nets which superseded Net 42 on 1 August 1947.

a. Normal Strip Systems.

(1) System No. 4701.

(a) Common normal strip system of Military Attaches in North and Latin America.

(b) Effective: 1 August 1947 -

(c) Distribution: All Military Attaches of North and Latin America.

---

*. Item in Index "Cryptonet 47", titled "Information and Records Section, MDAS-62: "Effective 1 August 1947, Cryptonet 42 (Military Attache) will be discontinued and replaced by three new Cryptonets to wit as follows: Cryptonet 47 - Western Hemisphere; Cryptonet 48 - Far East; Cryptonet 49 - Europe, Africa, Near East."

(d) Discussion: In Cryptonet 47, neither System No. 4701 nor any other strip system is used for messages classified higher than CONFIDENTIAL. If necessary for one Military Attache to communicate SECRET information to another, it must be relayed through WAR. (Use of one-time systems for communication between WAR and Military Attaches was continued in Net 47.

(2) System No. 4801.

(a) Common normal strip system of Military Attaches in Far East.

(b) Effective: 1 August 1947 -

(c) Distribution: All Military Attaches in the Far East Area.

(d) Discussion: (Use of one-time systems for communication between WAR and Military Attaches was continued in Net 47.)

(3) System No. 4901.

(a) Common normal strip system of Military Attaches in Europe, India, and Near East.

(b) Effective: 1 August 1947 -

(c) Distribution: All Military Attaches in Europe, Africa, and Near East.

(d) Discussion: (Continued use of one-time systems for communication between WAR and Military Attaches was continued in Net 47.)

b. Four-day Strip Systems. - None.

Cryptonet 17. (AIR FORCE AACS NET)

c. Normal Strip Systems.

(1) Only one normal strip system which was

(2) System No. 1763.

(a) Purpose of this system is to provide cryptographic communications [illegible]

of U. S. Army Air Forces and units of Royal Canadian Air Force.

(b) Effective: Sept. 1943 -

(c) Distribution: WD, Hq. AACS; AAF, Hq.; Air Transport Command; and AACS stations along Ferry Routes.

(d) Discussion: See (2)(a).

b. Stand-by Strip Systems.

(1) System No. 1721.

(a) Stand-by strip system for normal SIGABA System No. 1701.

(b) Effective: September 1943 -

(c) Distribution: WD, Hq. AACS; AAF, Hq.; Air Transport Command; and AACS stations along Ferry Routes.

(2) Systems No. 1722, 1723, [illegible]

(a) Stand-by strip system for normal SIGABA Systems No. 170[illegible], 1702, [illegible] 1708, 1709.

(b) Effective: September 1943 [illegible] which was effective [illegible] 194[illegible] -

(c) Distribution: WD, Hq. AACS; AAF, Hq.; Air Transport Command and AACS stations of one or two Ferry Routes.

(d) Discussion: System 1729 (and its complementary systems, 1709 and 1749) were issued to AACS Facilities along African Ferrying Route ([illegible] AACS Wing) to alleviate burden of excessive traffic load carried by the 1708, 1728, 1748 group. Before the addition of Systems 1709, 1729, 1749 to Net 17, Systems 1708, 1728, 1748 were used by AACS Facilities along the African and China, Burma, India Ferry Routes. With addition of the new Systems 1709, 1729, and 1749, Systems 1708, 1728, and 1748 were confined to use by AACS Facilities along China, Burma, India Ferry Routes.

9. Cryptonet 40. (World-wide Joint Army-Navy Cryptonet)

a. Formal Strip Systems.

(1) System No. 4022.

(a) Formal system for non-SIGABA holders.

(b) Effective date: 1 May 1945 -

(c) Distribution: System No. 4022 was, at first, the system of Cryptonet 40 designated for holders in the Pacific and Pacific Ocean Areas. This was true until 1 December 1946, at which time System No. 4022 superseded System No. 4023 and was henceforth used for world-wide communication instead of only in the Pacific Area.

(d) For System No. 4022 as stand-by, (see 9b(1).

(2) System No. 4023.

(a) Formal system for non-SIGABA holders.

(b) Effective date: 1 May 1945 - 1 December 1946.

(c) Distribution: Large number of Joint Army-Navy holders in Atlantic Ocean Areas only.

(d) Discussion: Superseded on 1 December 1946 by System No. 4022. For System No. 4023 as stand-by see 9b(2).

b. Stand-by Systems.

(1) System No. 4022.

(a) Stand-by strip system for normal SIGABA systems.

(b) Effective: 1 May 1945 -

(c) Distribution: Superseded System 11 in the Pacific. Large No. of Joint Army-Navy holders in Pacific and Pacific Ocean Areas until 1 December 1946 at which time it became world-wide.

(2) System No. 4023.

(a) Stand-by strip system for normal CIMRA systems.

(b) Effective: 1 May 1945 - 1 December 1946.

(c) Distribution: Large number of Joint Army-Navy holders in Atlantic Ocean Areas only.

(d) Discussion: Superseded on 1 December 1946 by System No. 4022. On 1 November 1945, use of System 133 was discontinued by Army units except those in the Greenland Area, and all traffic formerly passed in this system was henceforth passed in System 4023. System 133 remained in effect in the Greenland Area for special communication between Army and Navy headquarters.

10. Cryptonet 18.[9] (Alaskan Department and Northwest Service Command).

(1) System No. 1822.

(a) Normal strip system of Alaskan Department. (See Distribution.

(b) Effective: 1 October 1943 - 1 January 1946.

(c) Distribution: Various headquarters of Alaskan Department and Northwest Service Command and headquarters so designated by Alaskan Department.

---

9. The listing of systems of theater cryptonets according to the basic document does not give as accurate a picture as the listing of systems of world-wide cryptonets. This is true for two reasons: first, because modification of the systems, as issued by the theater by Army Security Agency, as designated by theater Headquarters and second, because the system were not necessarily used in the combinations designated by the basic documents.

(d) Discussion: The purpose of System No. 1822 was to include headquarters of Alaskan Department not holding SIGABA. Cryptonet 18 was discontinued 1 January 1945.

(2) System No. 1823.

(a) Normal strip system of Northwest Service Command. (See Distribution.)

(b) Effective: 1 October 1943 - 1 June 1945.

(c) Distribution: At first distributed to Alaskan Defense Command and Alaskan Highway Headquarters. Upon completion of Alaskan Highway, distribution, instead, included various other headquarters of Alaskan Department and Northwest Service Command and units designated by Northwest Service Command.

(d) Discussion: The purpose of System No. 1823 was to include units of Northwest Service Command not holding SIGABA. Accomplished questionnaires from holders indicated System 1823 was no longer needed and was, therefore, discontinued as of 1 June 1945.

b. Stand-by Strip Systems.

(1) Only one stand-by strip system which is

(2) System No. 1821.

(a) Stand-by strip system of Alaskan Department for normal SIGABA System No. 1 M.

(b) Effective date: 1 October 1943 - 1 January 1946.

(c) Distribution: Various headquarters of Alaskan Department; Headquarters, Northwest Service Command; HQ designated by Alaskan Department; and HQ, designated by Northwest Service Command.

(d) Discussion: For SIGABA holders only. Cryptonet 18 was discontinued 1 January 1946.

11. Cryptonet 19. (U.S.A. Forces in Middle East and Persian Gulf Command).

a. Normal Strip Systems.

(1) System No. 1922.

(a) Normal strip system of U.S.A. Forces in Middle East.

(b) Effective: 1 November 1943 - July 1944

(c) Distribution: U.S.A., Forces in Middle East, Middle East Service Commands; and other headquarters as designated by U.S.A., Forces in Middle East; Persian Gulf Command.

(d) Discussion: The purpose of this system was to include headquarters of Forces in Middle East not holding SIGABA. With the termination of the European phase of the War, the Africa-Middle East Theater had little use for Cryptonet 19 and Army Security Agency recommended to the Theater that it be discontinued. Concurrence from the Theater was received.

(2) System No. 1923.

(a) Normal strip system of Persian Gulf Command.

(b) Effective: 1 November 1943 - Fall 1944.

(c) Distribution: Persian Gulf Command and headquarters as designated by Persian Gulf Command.

(d) Discussion: In fall of 1944, System No. 1923 was superseded by Cryptonet 4., the newly formed Cryptonet for the Persian Gulf Command.

b. Stand-by Strip Systems.

(1) Only one stand-by system which is

(2) System No. 1921.

(a) Stand-by strip system of U.S.A. Forces in Middle East for holders of SIGABA System No. 1901.

(b) Effective date: 1 November 1943 -

(c) Distribution: U.S.A. Forces in Middle East; Middle East Service Commands and other headquarters designated by U.S.A. Forces in Middle East; Persian Gulf Service Command.

(d) Discussion: For SIGABA holders only.

12. Cryptonet 20. (Southwest Pacific Area)

a. Normal Strip Systems.

(1) Only one normal system which is

(2) System No. 2022.

(a) Normal strip system of SWPA.

(b) Effective date: 1 November 1943 - 1 January 1946.

(c) Distribution: CINC, SWPA; headquarters as designated by CINC, SWPA.

(d) Discussion: The purpose of System No. 2022 was to include headquarters of SWPA not holding SIGABA. Cryptonet 20 was discontinued, 1 January 1946, when the revised Cryptonet 40 superseded Cryptonets 20, 21, 23, 37, and 42.

b. Stand-by Strip Systems.

(1) Only one stand-by system which is

(2) System No. 2021.

(a) Stand-by daily system of SWPA for System No. 2001.

(b) Effective date: 1 November 1943 - 1 July 1946.

(c) Distribution: CINC, SWPA; headquarters as designated by CINC, SWPA.

(d) Discussion: For SIGABA holders only. Discontinued in July 1944 in accordance with radiogram [illegible] from Brisbane, Australia.

13. Cryptonet 21. (Pacific Ocean Areas)

a. Normal Strip Systems.

(1) Only one normal strip system which was

(2) System No. 2122

(a) Normal strip system in Pacific Ocean Areas.

(b) Effective date: 16 October 1943 - 1 January 1946.

(c) Distribution: Headquarters in Pacific Ocean Areas as designated by Headquarters, USAF in PAO.

(d) Discussion: See 13b(2) for System No. 2122 in its capacity as stand-by system. Cryptonet 21 was discontinued 1 January 1946, when the revised Cryptonet 45 superseded Cryptonets 20, 21, 23, 37, and 45.

b. Stand-by Strip Systems.

(1) System No. 2121.

(a) Stand-by strip system for normal SIGABA System No. 2101.

(b) Effective: 16 October 1943 - approx. April 1945.

(c) Distribution: U.S.A. Forces in South Pacific and headquarters designated by U.S.A. Forces in South Pacific.

(d) Discussion: Discontinued (approx. April 1945) when System No. 2122 became stand-by for System No. 2101. See 13b(2) in its capacity as a stand-by system.

(2) System No. 2122.

(a) Stand-by strip system for normal SIGABA System No. 2101.

(b) Effective as stand-by system: approx. April 1945 - 1 January 1946.

(c) Distribution: Headquarters in Pacific Ocean Areas as designated by Headquarters, USAF in PAO.

(d) Discussion: Became stand-by system for SIGABA System No. 2101 when stand-by System No. 2121 was discontinued.

(3) System No. 2125.

(a) Strip system. Basic document does not state whether stand-by or normal. It was probably a stand-by for normal SIGABA System No. 2105. May have also had a normal status.

(b) Effective: Approx. April 1945 - 1 January 1946.

(c) Distribution: Special headquarters in Pacific Ocean Areas as designated by Headquarters, USAF in PAO.

(d) Discussion: For tactical operations only.

Component 22. (European Theater).

a. Normal Strip Systems.

(1) Only one normal strip system which is

(2) System No. 2202.

(a) Normal strip system at Washington D. C. for units not authorized SIGABA until 1 September 1947 after which it becomes the normal strip system for units not authorized SIGABA.

[illegible] System No. 201, effective [illegible] the general replacement of SIGABA by SIGCUM in the European Area on 1 September 1947, Cryptoprotek 2202, presently employed in the Mediterranean Area only, will be extended for use through the European Area, replacing SIGABA System 2201. At the same time, the High Command System 2207 will be superseded by System 2201, SIGABA machines and associated material in the Mediterranean Area until 1 November 1947. At that date, [illegible] European Command will be the only unit in that area authorized to hold SIGABA machines and System No. [illegible]

(b) Effective date: 10 October 1943 -

(c) Distribution: HQ in ETO as designated by HQ, ETO.

(d) Discussion: See below for System No. 2222 in its capacity as a stand-by system.

b. Stand-by Strip Systems.

(1) System No. 2221.

(a) Stand-by strip system for normal SIGABA system No. 2101.

(b) Effective date: 10 October 1943 - 1 January 1946.

(c) Distribution: HQ in ETO as designated by HQ, ETO

(d) Discussion: Discontinued 1 January 1946 when System No. 2222 became stand-by for System No. 2101. (See 1b(2) for System No. 2222 in its capacity as stand-by system.

(2) System No. 2222.

(a) Stand-by strip system for normal SIGABA System No. 2201 from 1 January 1945 - 1 September 1947. On 1 September 1947, it became, instead, stand-by for normal SIGROD System No. 2213.

(b) Effective as stand-by system: 1 January 1946

(c) Distribution: HQ in ETO as designated by HQ, ETO.

(d) Discussion: The change from stand-by for SIGABA System No. 2201 to stand-by for SIGROD System No. 2213 occurred when SIGROD replaced SIGABA in the European Theater Cryptonet 22. It retained its status as

---

1502, 4001, 4002, and 4005... Cryptosystem 2222 will continue as the normal system for those units not authorized SIGROD and will also serve as a backup system for Allied... Fellow Items Interoffice (Compromises), Information and Records Subsection, MIDAS-62.

general alphabet strip system, thus serving in dual capacity as normal and stand-by system.

15. Cryptonet 23. (Asiatic Theater)

a. Normal Strip Systems.

(1) Only one normal strip system which was

(2) System No. 2322.

(a) Normal strip system of ATO.

(b) Effective date: 1 October 1943 - 1 January 1945.

(c) Distribution: Headquarters in ATO as designated by HQ, ATO.

(d) Discussion: See below for System No. 2322 in its capacity as a stand-by system. Cryptonet 23 was discontinued 1 January 1945, when the revised Cryptonet 45 superseded Cryptonets 20, 21, 23, 37, and 45.

b. Stand-by Strip Systems.

(1) System No. 2321.

(a) Stand-by strip system for normal SIGABA System No. 2301.

(b) Effective date: 12 September 1943 - January 1945.

(c) Distribution: Headquarters in ATO as designated by HQ, ATO.

(d) Discussion: Discontinued January 1945 when System No. 2322 became stand-by for System No. 2301. See 15b(2) for System No. 2322 in its capacity as stand-by system.

(2) System No. 2322

(a) Stand-by strip system for normal SIGABA System No. 2301.

(b) Effective date as stand-by system:

January 1945 - 1 January 1946.

(c) Distribution: HQ in ATO as designated by HQ, ATO.

(d) Discussion: Became stand-by system for normal SIGABA System No. 2301 when stand-by System No. 2321 was discontinued. In July 1945, the India Theater changed System No. 2322 from a semi-monthly supersession basis to a monthly supersession basis.

16. Cryptonet 24. (Mediterranean Theater)

a. Normal Strip Systems.

(1) Only one normal strip system which was [11]

(2) System No. 2422.

(a) Normal strip system of Allied Force. [11]

(b) Effective: 1 December 1943 -

(c) Distribution: Allied Force Hq. and headquarters as designated by Allied Force Hq.[11]

(d) Discussion: For use of System No. 2422, see footnote 11 below and "Discussion under System No. 2421.

b. Stand-by Strip Systems.

(1) Only one stand-by strip system which was

(2) System No. 2421.

(a) Stand-by strip system of Allied Force for normal SIGABA System No. 2401.

(b) Effective date: 1 December 1943 - January 1945.

---

11. Letter, subject: Revision of Cryptonet 24", 3rd Ind., From: Signal Officer, Hq. Allied Force; To: CCSLO 10 November 1944. "...strip System No. 2422 was issued for some months for special purpose AF Force aircraft since the system was serving no other purpose. The need for the special system no longer exists and no more than one strip system is required in Cryptonet 24". Folder File 2308 (Allied Force), 8-1-44 - 9-30-44.

(c) Distribution: Allied Forces Headquarters.

(d) Discussion: After a long period of negotiation with MTO, it was finally decided to discontinue Systems No. 2421 and 2441. They then used 2422 as their normal strip system and 2441 as emergency DT, effective for a period of 6 months.[12]

17. Cryptonet 26.

a. Normal Strip Syatems.

(1) System No. 2621.

(a) Normal strip system.

(b) Effective date: September 1943 - December 1944.

(c) Distribution: Antilles Air Task Force; U.S.N.A. Cuba; U.S.N.A. Haiti; U.S.N.A. Dominican Republic; Puerto Rican Dept.

(d) Special holders as listed.

b. Stand-by Strip Systems. - None.

18. Cryptonet 27. (Caribbean Area)

a. Normal Strip Systems.

(1) Only one normal system which was

(2) System No. 2722.

(a) Normal strip system for holders not authorized SIGABA.

(b) Effective date: 1 March 1945 - 1 March 1946.

(c) Distribution: Caribbean Defense Command; Antilles Dept.; Puerto Rican Sector; Hq. as designated by Puerto Rican Sector; Trinidad Sector and Base Command; Hq. as designated by Trinidad Sector and Base Command; Panama Canal Department.

---

12. Interoffice Memo No. 101, from Major T. R. Chittenden, 21 January 1943, Holden, Interoffice News (Compromise), Information and Records Subsection, Communications Section, Security Division (OSCAB-WD).

(d) Discussion: When Net 27 was discontinued 1 March 1946, holders of System No. 2722 were furnished System No. 1501 to prevent impairing communications by discontinuing the Net.

b. Stand-by Strip Systems.

(1) System No. 2721.

(a) Stand-by strip system for normal SIGABA System No. 2701.

(b) Effective: 1 March 1944 - approx. April 1945.

(c) Distribution: Same as distribution of System No. 2722.

(d) Discussion: Discontinued (approx. April 1945) when System No. 2722 became stand-by for System No. 2701. See below for System No. 2722 in its capacity as a stand-by system.

(2) System No. 2722.

(a) Stand-by strip system for normal SIGABA System No. 2702.

(b) Effective as stand-by system: approx. April 1945 - 1 March 1946.

(c) Distribution: Hq., U.S.A.F.E.A.; Hq., Caribbean Defense Command; Hq., Antilles Dept.; Hq., Panama Canal Dept.; Hq., 8th AACS Wing; Miami Signal Center.

(d) Discussion: Became stand-by system for SIGABA System No. 2702 when stand-by System No. 2721 was discontinued. Net 27 discontinued 1 March 1945.

10. Cryptonet 29.

a. Normal Strip Systems.

(1) System No. 2921.

(a) Normal strip system for all holders of Cryptonet 29.

(b) Effective: 1 January 1944 - 1 June 1945.

(c) Distribution: 30 holders. Difficult to categorize without listing holders.

(d) Discussion: System No. 2921 is the common normal system for all holders of Cryptonet 29. Only two systems are held in Cryptonet 29, the other being the emergency DT system for System No. 2901.

b. Stand-by Strip Systems. - None.

20. Cryptonet 30. (Asiatic Theater)

a. Normal Strip Systems. - None

b. Stand-by Strip Systems.

(1) Only one stand-by strip system which was

(2) System No. 3021.

(a) Stand-by strip system for normal STOAEA System No. 3001.

(b) Effective: 16 December 1939 - 1 June 1940.

(c) Distribution: WD: AMC, Mon Wehdi; US as designated by AMC, New Delhi.

(d) Discussion: Only three systems held in this cryptonet: Normal STOAEA system, emergency DT system, and stand-by strip system No. 3021.

21. Cryptonet 31. (Headquarters Curphonet).

a. Normal Strip Systems. - None

b. Stand-by Strip Systems.

(1) System No. 3121.

(a) Stand-by strip system for normal STOAEA System No. 3101.

(b) Effective date: 21 October 1939 - April 1940.

(c) Distribution: WD: U.S.A. Forces in Southwest Pacific Islands Number 2

Operations; U.S.A. Forces in South Pacific European Theater of Operations; Allied Forces HQ, Algiers.

(d) Discussion: The systems of Cryptonet 31 were held at the headquarters listed under "distribution" and were not distributed to any other headquarters within the theater. Strip systems of Cryptonet 31 were discontinued approx. April 1945. Cryptonet 31 was discontinued Oct. 1945.

(2) Systems No. 3122, 3123, 3124, 3125, 3126.

(a) Isolation stand-by strip systems for normal SIGABA Systems No. 3101, 3102, 3103, 3104, 3105, 3106, respectively.

(b) Effective date: 25 October 1943 - April 1945.

(c) Distribution: Each system listed held by HD and one individual headquarters, listed under Distribution of System No. 3121 in subparagraph (1) above.

(d) Discussion: Isolation stand-by strip systems for communication between HD and the individual holder. Strip systems of Cryptonet 31 were put on a quarterly supersession basis, 15 September 1944, and were discontinued April 1945. Cryptonet 31 was discontinued October 1945.

22. Cryptonet 32.

a. Normal Strip Systems.

(1) Only one normal system which was

(2) System No. 3222.

(a) Normal strip system for non-SIGABA holders.

(b) Effective date: October 1943 -

(c) Distribution: AFHQ, Naples, Italy; Eq. as designated by AFHQ, Naples, Italy.

(d) Discussion: For non-SIGABA holders.

b. Stand-by Strip Systems.

(1) Only one stand-by strip system which was

(2) System No. 3221.

(a) Stand-by strip system for normal SIGABA System No. 3201.

(b) Effective date: October 1943 -

(c) Distribution: AFHQ, Naples, Italy; Eq. as designated by AFHQ, Naples, Italy.

55. Cryptonet 55. (Special Security Officer's Cryptonet)

a. Normal Strip Systems. - None.

b. Stand-by Strip Systems.

(1) System No. 3321.

(a) Stand-by strip system for normal SIGABA System No. 3301.

(b) Effective date: 2 November 1943 - February 1945.

(c) Distribution: Security officers at: HQ, U.S.A. Forces in Southwest Pacific Asiatic Theater of Operations; U.S.A. Forces in Central Pacific.

(d) Strip systems of Cryptonet 55 were discontinued in February 1945, after which time other high grade system held at HQ where Security Representatives were located were used if systems of Net 55 became inoperative. On 1 January 1948 Net 55 will be superseded by System 990, a SIGTOT system.

(2) Systems No. 3322, 3323, 3324, 3325, 3326.

(a) Isolation stand-by strip systems for normal SIGABA Systems No. 3302, 3303, 3304, 3305, respectively.

(b) Effective date: Fall 1943 - approx. April 1945.

(c) Distribution: Each system listed held by HD and one of the individual headquarters listed under Distribution of System No. 3321.

(d) Discussion: Isolation stand-by systems for communications between WAR and the individual holder. Strip systems of Net 55 were discontinued 1 April 1945.

24. Cryptonet 39. (Special Cryptonet for 20th Air Force)[17]

a. Normal Strip Systems. - None.

b. Stand-by Strip Systems.

(1) System No. 3921.

(a) Stand-by strip system, probably both for normal SIGABA System No. 3901 and normal SIGGUM System No. 3902.

(b) Effective date: 1 December 1944 - 1 January 1946.

(c) Distribution: HD (CG 20th Air Force) and other AF units with which it was necessary for 20th Air Force to communicate.

(d) Discussion: Strips were used entirely as stand-by means of communications in Cryptonet 39. One ABA system and four CSM systems held by various holders. Cryptonet 39 was discontinued on 1 January 1946.

(2) Systems No. 3923, 3924, 3925.

(a) Stand-by strip systems for normal SIGGUM Systems No. 3903, 3904, 3905, respectively.

(b) Effective date: 1 December 1944 - 1 January 1946.

(c) Distribution: 5 holders of each system for communication within and between 20th, 21st, and 22nd Bomber Commands.

(d) Discussion: Cryptonet 39 was discontinued 1 January 1946.

---

17. Letter, Subject: Cryptographic Systems for Twentieth Air Force, From: J. M. Carroll, Major, Air Corps, Chief, Cryptographic Branch, Communications Control Division, Office of Air Communications Officer. To: CSO, Attn. Major Russell H. Horton. Folder, "Cryptonet 39", Information and Records Subsection, Administrative Section, Security Division (CSGIS-90).
"...In order that security requirements of communications may be adequately met, it is necessary that a separate Cryptonet for use by the Twentieth Air Force be prepared."

25. Cryptonet 41. (Persian Gulf Command). - Superseded System No. 1923 of Cryptonet 19.

a. Normal Strip Systems. - None.

b. Stand-by Strip Systems.

(1) Only one stand-by strip system which was

(2) System No. 4122.

(a) Stand-by strip system for normal SIGABA System No. 4101 and normal SIGFOY System No. 4102.

(b) Effective date: 1 January 1945 -

(c) Distribution: Persian Gulf Command and headquarters as designated by Persian Gulf Command.

(d) Discussion: Cryptonet 41 replaced System No. 1923, thereby giving Persian Gulf Command a cryptonet of its own instead of combining it with U.S.A. Forces in Middle East. See Cryptonet 19 (Item 11, Cryptonet 19). A message from Cairo (MI 55234, 11 December 1945) stated that the Persian Gulf Command was being inactivated and, effective 21 December 1945, held only System 4122 for cryptographic communication until complete deactivation.

26. Cryptonet 42. (CINCAFPAC; POA; SWPA)

a. Normal Strip Systems. - None.

b. Stand-by Strip Systems.

(1) Only one stand-by strip system which is

(2) System No. 4521.

(a) Stand-by strip system for Cryptonet 45.

(b) Effective date:

(c) Distribution: CINCAFPAC and Hq as designated by CINCAFPAC.

(d) Discussion: Revised Cryptonet 42 superseded, on 1 January 1946, Cryptonets 20, 21, 43, 37, and 45. System 4521 was added to Cryptonet 45 on 1 January 1946.

27. Cryptonet 10. (Training Net) - Systems No. 1021, 1022, 1023, 1024, 1025, and 1026 were the alphabet strip systems used for training. Effective from about May 1943 through November 1944, at which time Cryptonet 10 was superseded by Training Cryptonets 97, 98, and 99. Cryptonet 98 was issued to Fort Monmouth for training; Cryptonet 99 was issued to Camp Crowder for training; and Cryptonet 97 was issued for communication between the two. Cryptonet 10 held for training, besides the strip systems listed, systems of all other widely used means of cryptographic communication.

28. Cryptonet 98. - One of the three training nets which superseded Cryptonet 10. Issued to Fort Monmouth and headquarters designated by Fort Monmouth. System No. 9822 was the strip system of Cryptonet 98 authorized as the training system for strips. Cryptonet 98 became obsolete on 1 May 1946.

29. Cryptonet 99. - One of the three training nets which superseded Cryptonet 10. Issued to Camp Crowder and headquarters as designated by Camp Crowder. System No. 9922 was the strip system of Cryptonet 99 authorized as the training system for strips. Cryptonet 99 became obsolete on 1 May 1946.

30. Cryptonet 97 - One of the three training nets which superseded Cryptonet 10. Issued for communication between holders of Cryptonets 98 and 99. System 9722 is the strip system of Cryptonet 97 authorized as the training system for strips. After Cryptonets 98 and 99 became obsolete on 1 May 1946, Cryptonet 97 continued on a quarterly supersession schedule and was used for "live traffic" training at Camp Crowder and Fort Monmouth. On 12 March 1946 (per I.C.M. 372; certain editions of Cryptonet 97 were designated as permanent training editions. This list included the strip system edition 9722-18.

MAJOR CHANGES IN THE USE OF

STRIP CIPHER DEVICES

as illustrated by changes affecting security which appeared in the following instructional documents concerning strip cipher devices:

"Instructions for Using Strip Cipher Devices" (short title: SIGUHR), April, 1942. Obsolete.

"Instructions for Using Strip Cipher Devices" (short title: SIGUHR-2), April, 1943. Obsolete.

"Instructions for Using Strip Cipher Devices" (short title: SIGUHR-3), March, 1945. Obsolete.

"Instructions for Using the Strip Cipher Device" (short title: SIGUHR-4), July, 1946.

	SIGHUR April 1943	SIGHUR-2 1 July 1943	SIGHUR-3 1 March 1943	SIGHUR-4 1 July 1946
Numbers and Names of Devices in Use	3 devices in use: M-138 M-138-A CSP 845	4 devices in use: M-138 M-138-A CSP 845 SIGWOOD	3 devices in use: M-138-A (aluminum) CSP 845 (aluminum or plastic) SIGWOOD (wooden)	1 device in use: CSP 845 (aluminum)
Channel elimination — Strip elimination	Messages classified SECRET (except joint Army-Navy messages) make use of channel elimination. Messages classified CONFIDENTIAL do not [illegible] the channel elimination [illegible]. All 30 [illegible] [illegible], i.e., 15 [illegible] [illegible] [illegible] (top half of device), and [illegible] 15 [illegible] are taken from another [illegible] (bottom half of device).	Messages classified SECRET and, usually messages classified CONFIDENTIAL make use of channel elimination.	Channel elimination is used with all messages.	Strip elimination is used with all messages.

	SIGUHR	SIGUHR-2	SIGUHR-3	SIGUHR-4
	When channel elimination is used, 5 channels are always eliminated.	When channel elimination is used 5 channels are always eliminated. Change to SIGUHR-2, Sept. 1944: Total number of channels eliminated may be any number from 1-5 will be eliminated. (Repetitions of numbers occur because, according to new system, the 5 numbers indicating the channels to be eliminated will be found on 5 consecutive lines of the channel elimination grid instead of on the same line. Blanks appear on every line except the fifth.	Some variation in number of channels as per change to SIGUHR-2; some method of determining numbers for the elimination.	Some variation in number of eliminations; some method of determining numbers for the elimination as in SIGUHR-3. However, numbers in the elimination table for the first time refer to strip numbers instead of to the channel number.

	SIGGUE	SIGGUE-2	SIGGUE-3	SIGGUE-4
	5 different letters are selected at random for the message indicator.	Still specifies 5 different letters for message indicator.	Still specifies 5 different letters for message indicator.	Any 5 letters chosen at random may be used for the message indicator. Repetitions may occur by chance.
Selection of same generatrix	A deliberate attempt should be made to prevent the selection of columns the same distance from the plain-text column in enciphering a long message.	Never select the same generatrix twice.	Never select the same generatrix twice.	Never select the same generatrix twice.
Completion of last group	Use plain-text X's to complete last group	Use plain-text X's to complete last group	Use plain-text X's to complete last group.	To complete last group encipher either X or Z once and then, if necessary, encipher enough different nulls to complete the last group. This change is made possible by encipherment.

~~SECRET~~

CHRONOLOGY OF CHANGES RELATING TO CHANNEL ELIMINATION

AND SPLIT GENERATRIX

Before 1939 - Use of 25 strips with no interruptor scheme of encipherment.

July 1939 - Introduction of channel elimination into only Systems 2& and 6. Gradual introduction of channel elimination into other systems until January 1942.

Jan. 1942 - Introduction of "split generatrix" for CONFIDENTIAL messages and channel elimination for SECRET messages.

July 1943 - After this date channel elimination was used for all messages classified SECRET and most messages classified CONFIDENTIAL. Only a few CONFIDENTIAL systems were not provided with channel elimination tables and, therefore, retained "split generatrix" procedure.

Sept. 1944 - Introduction of variable number of channels eliminated in each message. (Split generatrix procedure completely eliminated by this time.)

July 1945 - Introduction of elimination by strip number instead of channel number.

~~SECRET~~

REFERENCE FILES

OFFICE OF THE CHIEF SIGNAL OFFICER
Engineering and Technical Services, The Pentagon.
Minutes of Signal Corps Technical Committee Meetings

Files of Nomenclature Section, The Pentagon

WAR DEPARTMENT, RECORDS BRANCH (219 N. Lee St., Alexandria, Va.)
File: 461 (M-94) Cipher Device No. 1, 1921- (obs. 1945)

NATIONAL ARCHIVES
War Department Code and Cipher Section
File: 311.5 Codes

ARMY SECURITY AGENCY LIBRARY
Articles on Cryptography and Cryptanalysis, "Edgar Allan Poe, Cryptographer", William F. Freidman, 1942.

Several Machine Ciphers and Methods for their Solution, "A Multiplex Alphabet System", Publication No. 20, Riverbank Laboratories, (1918).

OFFICE OF CHIEF COMMUNICATIONS RESEARCH SECTION (OSGAS-14)
File: Cipher Device M-138 and M-138-A

SECURITY DIVISION (OSGAS-80)
Methods Branch, Analysis Section, Literal Systems Subsection,
Strips, Volume I and II

Material Branch, Registered Publications Section,
Item Cards, re Distribution of Strip Systems

Administrative Section, Information and Records Subsection,
File: Cipher Device M-94.
File: Cipher Device M-138.
File: Cipher Device M-138-A.
File: Cipher Device CSP 845.
File: Cryptonets.
File: Interoffice Memorandum.
File: Systems.
File: Trip Reports.

SPECIFICATIONS

Cipher Device M-94		
No. 72-26	20 May 1921	
72-26-A	1 Mar 1926	(Approved by SCEC)
Cipher Device M-138		
No. 71-716	28 Sep 1954	Cancelled Dec 1954
71-716-A	24 Nov 1954	Cancelled Dec 1954
71-716-A	7 Jan 1955	
Cipher Device M-138-A		
No. 71-716-B	7 Apr 1958	
Amendment No. 1	17 Apr 1958	
Annex Issue No.7	25 Oct 1940	

NOMENCLATURE

M-136	15 Jun 1955	Nomenclature Sec., Supply Div., OCSigO
M-137	17 Aug 1955	Nomenclature Sec., Supply Div., OCSigO
M-138	26 Aug 1955	Nomenclature Sec., Supply Div., OCSigO
(All three requested by War Plans and Training Div., OCSigO)		
M-138-A	8 Jun 1957	Nomenclature Sec., Supply Div., OCSigO
(Requested by Research and Development Div., OCSigO)		

OPERATING INSTRUCTIONS

	Feb 1922	Instructions for Using Cipher Device M-94	Obsolete
SIGSOB	1935	Instructions for Cipher Device Type M-138	"
SIGCUM	1939	Instructions for Cipher Device M-138 and M-138-A	"
SIGCUM	1940	Instructions for Cipher Device M-138 and M-138-A (Revised)	"
SIGCUM	Apr 1942	Instructions for Using Strip Cipher Device	"
SIGCUM-2	Apr 1945	Instructions for Using Strip Cipher Device	"
SIGCUM-3	Nov 1945	Instructions for Using Strip Cipher Devices	"
SIGCUM-4	Jul 1946	Instructions for Using the Strip Cipher Device	

[redacted]

SECURITY REPORTS*
(Filed in CSGAS-83, Analysis Section,
Literal Systems Subsection)

VOLUME I.

7000.1 - Lecture on Strip Systems.
7000.2 - Frequency of Strip Cipher Text Based on 31 Messages - 13,617 Letters.
7000.3 - Report on the Proposed Revision of the Strip Cipher Device.
7000.4 - Time Required for Setting-up and Tearing-down a Strip Cipher Device.
7000.5 - Reconstruction of Flat Strip System: Compromise of Plain and Cipher Text (48 groups).
7000.6 - Modified Strip System and Comparison of Frequency Distribution of Cipher Equivalents using Converter M-134-C and a 100-Strip System.
7000.7 - Identification of Strip and Machine Cipher Systems.
7000.8 - Report on Signal Corps Board Case No.193, Cipher Device, Type M-138.
7000.9 - Chronological List of Data Re M-138
7100.1 - Cryptanalysis of the Strip System.
7110.1 - Cryptanalysis of Star Cipher.
7130.1 - Navy Method of Solution of the Cylindrical Cipher Device (CSP-488).
7130.2 - Indirect Method of Solution for Strip Ciphers (Approximate Theory).
7121. - Excerpts from Correspondence Re M-94 (M. Rhoads & W.F. Friedman).
7121.1 - Proposal for Modifying Cipher Device M-94.
7121.2 - Cryptographe Cylindrique (Re M-94 & Transposition).
7122.1 - M-94 (System Unknown).
7122.2 - Breaking down Cipher Device Messages (M-94).
7122.3 - A method of Determining Identical Generatrices in Cryptograms of the Type Produced by Cipher Device, Type M-94.
7123.1 - M-94 (System Unknown).
7131.1 - A 15-Alphabet Strip Cipher System.
7131.2 - Solution of M-138.
7132.1 - System 56 Security Study.
7132.2 - Report of a Test of the Security of System 56-1.
7132.3 - System 56 Security Study Continued.
7132.4 - System 56 - Problem III.
7132.5 - An Analysis of System 56.
7140.1 - Authentication System AFHQ.
7140.2 - Detailed Report of the Methods used in Analysis of Authentication System AFHQ (with Modification).

VOLUME II.

7210.1 - Preliminary Report on Determination of Number of Strips Eliminated.
7210.2 - Determination of Number of Alphabets used in Messages Enciphered in a Strip System.
7210.3 - Strip Systems (Channel Elimination).
7211.1 - Analysis of the Security of System 6.
7211.2 - Report on the Study of the Security of System (Strip System).
7211.4 - Report on the Study of the Security of Channel-Elimination Strip Systems.
7211.5 - Study of Cryptographed Traffic from the United States Military Attache, Bern, Switzerland.
7211.1 - Report on the Study of Navy Strip System---CSP-1154(N).
7211.2 - Study of Strip Elimination Table.
7211.3 - Study of Strip Elimination Table (II).
7240.4 - Key Lists for Strip Ciphers.

*These security reports appear in two volumes. The numbering system given is that used as a locator within the two volumes.

[redacted]

SECRET

HEADQUARTERS
ARMY SECURITY AGENCY
WASHINGTON 25, D.C.

8 February 1946

WDGSS-81

SUBJECT: Cryptographic Assistance Furnished Outside Agencies by the Army Security Agency

TO: Chief, Security Division

1. During the war the Security Division provided cryptographic assistance through its productive and technical facilities to the following governmental agencies:

Civil Aeronautics Administration
Division of Territorial and Island Possessions, Interior Department
Interservice Radio Propagation Laboratory
Federal Communications Commission
Office of Strategic Services
Office of War Information
Office of Scientific Research and Development
Petroleum Administration for War
Rubber Development Corporation
State Department
United Nations Relief and Rehabilitation Administration

2. This assistance fell into two categories:

a. Preparation and issue of cryptographic material and/or equipment designed to meet the cryptographic communications requirements of the respective agencies.

b. Advice to the agencies on cryptographic operations and procedures.

3. Since the end of the war, the amount of work done by the Security Division in supplying outside agencies with cryptographic assistance has decreased considerably, however, such assistance as is necessary is still rendered these agencies upon request.

4. The following is a resume of the general type of cryptographic material supplied outside agencies by Army Security Agency.

a. Civil Aeronautics Administration — strip systems for a very limited amount of traffic. Last provided in April 1944. War Department Telegraph Code was recommended for their type of communication but was never issued owing to the end of the war.

SECRET

b. Interior Department — strip systems provided for communication within division of territorial and island possessions. Last issued in June 1945. This system is used for traffic between Washington Headquarters, Puerto Rico, Alaska, Hawaiian Islands and Virgin Islands.

c. Interservice Radio Propagation Laboratory — Double transposition cipher and twenty-two editions of special subtractor pads were provided for isolated IRPL stations. Since the end of the war need for transmission of IRPL traffic in cipher does not exist, therefore this agency should no longer require services of the ASA.

d. Federal Communications Commission — strip system and total of 140 one-time pads provided. Last sent out in October 1945 and as far as is known is sufficient material to cover their current requirements.

e. Office of War Information — during the war, loop tapes, DT systems, with instructions, and pin and lug settings for the M-209 were provided. However, the OWI has recently been disbanded and the bulk of its responsibilities transferred to the State Department.

f. Office of Scientific Research and Development — strips were originally provided but were superseded by one-time pads. Later Army SIGTOT facilities were used for transmission of OSRD traffic.

g. Petroleum Administration for War — loop tapes for M-131 equipment were provided, but this agency was disbanded VJ Day.

h. Rubber Development Corporation — strip cipher system provided but this agency also has no further need for material.

i. United Nations Relief and Rehabilitation Administration — This agency is one of the few whose requirements have not decreased since the end of the war. Special instructions for use of the M-209 were provided along with several editions of M-209 systems. Also provided are several one-time pads with instructions. Additional editions of pads and M-209 systems are furnished upon request from UNRRA.

j. State Department — This organization has its own Security Division set up charged with the responsibility of supplying State Department units with cryptographic material. However, this Agency has continued to help out in furnishing necessary cryptographic material whenever so requested.

During the war, thousands of SIGHOY devices with motors and accessories associated with the SIGHOY were furnished the State Department; however, use of this gadget has been nearly discontinued, thus there should be little demand for further supply of this material. The same thing applies to SIGHASE which was also issued the State Department for use in connection with the SIGHOY project.

The State Department has set up a SIGTOT network for which the Army has supplied all the one-time tapes. The tape production facilities of this Agency were devoted almost entirely for three months to State Department requirements.

~~SECRET~~

Also approved the State Department at three-year intervals upon their request are stock strips and other types of raw scrambles which the State Department utilizes in making its own cryptographic systems.

c. Office of Strategic Services - Up until October 1945, the OSS was created as a non-military agency. On that date, OSS, as such, was disbanded and the Strategic Services Unit was set up directly under the Secretary of War. While the agency was OSS, the following cryptographic material was furnished:

(1) Strip cipher system in 1944.
(2) M-134A machines and associated systems.
(3) CCM and associated motors and systems which completely replaced the M-134A in October 1945.
(4) A very limited number of SIGCUM, SIGABA, and SIGTOT facilities which were made available to OSS through crypt teams within theaters of operation.

When OSS converted to SSU, the ASA assumed the responsibility for furnishing all cryptographic requirements for that agency. This entailed production of one-time pads in tremendous quantities since the one-time pad is the method or means of communication among the majority of SSU field units. Most of the one-time pads now produced by Security Division are for SSU. The production of the seventeen associated with the Combined Cipher Machine for SSU has continued.

d. White House - In addition to the above cited agencies, Security Division also furnishes cryptographic material for the Whitehouse Signal Detachment. This Detachment is under the command of an army officer but does communications security work for the President. The material furnished consists of a cryptonet made up of some SIGABA systems and two SIGTOT systems. Supply and accounting is handled in the same manner as regular War Department cryptographic material.

William A. Fleming, Jr.
Captain, Sig C

~~SECRET~~

SAVE

HEADQUARTERS
ARMY SECURITY AGENCY
WASHINGTON 25, D. C.

WDGSS-82

8 February 1946

TO: CHIEF, SECURITY DIVISION

SUBJECT: Work for outside agencies

In compliance with a request from Security Division for a list of work produced by Materiel Branch for outside agencies, the following list is submitted.

OWI	Tapes CKL No. 1075, D.T. CKL No. 10, Strip (1942)
OSRD	CKL No. 1, Strip (Jan 44) superseded by CS No. 954 (Pad system)
EDC	CS No. 4 including CKL No. 4-1, Strip (June 1945)
CAA	CS No. 52 including CAA CKL No. 52-1, Strip (April 45)
UNRRA	CS Nos. 500 including CKL No. 500-3 M-209 (Aug 45) 600 including CKL No. 600-3 M-209 (Aug 45) 700 including CKL No. 700-3 M-209 (Aug 45)
FCC	CS No. 47 including FCC CKL No. 47-1, Strip (Aug 45)
FCC/FCC	140 Literal One-Time Pads
FBI	CS Nos. 7 including CKL No. 7-1, Strip (May 45) 8 including CKL No. 8-1, Strip (May 45) 9 including CKL No. 9-1, Strip (May 45) 10 including CKL No. 10-1, Strip (May 45)
PAW	Tapes (1945)
OSS	CS No. 600-5
OSS	Keying Table No. 500-12, M-134-A CKL No. 84, Strip (May 44)
BSU	812 One-Time Pads
[illegible]	9,260 Tapes (11 Sep 45 - 7 Jan 46) Strip [illegible]

270

SOI and CINCPOA-CINCSWPA COVERS for the Conferences at Yalta, Quebec, Teheran (OCSIGO)

Covers for the visit of Prague and Blamey of Australia (OCSIGO)

Overprint of certificates of merit for SAF and ASF

At present only four of the above systems remain on the production schedule. The percentage of time and the number of man-hours per week for each system are:

OSS CS No. 600	1%	2 hours
SSU One-Time Pads	35%	176 hours
State Dept. Tapes	75%	150 hours
State Dept. Strip Systems	12%	35 hours

L. M. Myers
Lt. Colonel, Sig. Corps
Chief, Material Branch

[redacted]

ROUTING AND WORK SHEET

(PAR. 40.62 O.R.)

SUBJECT Cryptographic material for Civil Aeronautics Authority

Number each action	To—	Memorandum	Name, Division or Branch, and Date
1.	Major Chittenden	1. Mr. McCree has agreed to have CAA officials in Anchorage contact the Alaskan Theater Signal Officer and make arrangements to facilitate the use of CAA strip systems. 2. In anticipation of the results of this contact CAA has requested the following additional cryptographic material: a. 4 additional copies of CAA SECRET strips and key list. b. 4 additional copies of CAA CONFIDENTIAL strips and key list. c. 4 additional devices CSP-845. 3. Mr. McCree has scheduled a trip to Anchorage on the 28th of December and if the above material could be delivered on or before the 24th its transmission would be greatly expedited.	James G. Noak Captain, Sig. C. 14 December, 1943
2.	Captain Noak	Pursuant to conversation held jerkily this morning it is understood that this R & W, subject: "Cryptonet material for Civil Aeronautics Authority" has been superseded by word of mouths and hence will be henceforth ignored.	Thomas R. Chittenden Major, SPSIC-2 15 December 1943 Ext. 269
	Noted	agreed to send 17 copies of 2 new systems instead —	

SC104T

[redacted]

72

[redacted] (C-8401

BUY WAR BONDS

HEADQUARTERS, ARMY SERVICE FORCES
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON 25, D. C.

SPSIC 1 June 1945

SUBJECT: Issuance of SIGARM to the Civil Aeronautics Administration

TO: Assistant Chief of Staff, G-2
War Department General Staff
Washington 25, D. C.

1. The Civil Aeronautics Administration has requested a cryptographic system to be used within the continental limits of the United States for RESTRICTED messages. Such a cryptographic system would be employed by approximately ten stations for traffic consisting of a small number of messages sent at infrequent intervals. Issuance of the Converter M-209 or of a strip cipher system for this purpose is considered to be impractical because of the infrequent use to be made of the system.

2. A code book is considered to be the most satisfactory solution for the requirement, and it is felt that the War Department Telegraph Code, 1942 (short title: SIGARM) would be suitable for this purpose. Sufficient quantities are available to supply the Civil Aeronautics Administration with the code by 15 June 1945.

3. It is recognized that the issuance of SIGARM to the Civil Aeronautics Administration would theoretically enable a nonmilitary organization to read military traffic encoded in a War Department system. However, it is believed that the level of classification of this code and the ease with which such traffic could have been read in the past by any interested party would outweigh any objection on this ground. Steps are now being taken to replace SIGARM with a RESTRICTED strip cipher system on or about 1 August 1945 for use throughout the Army.

4. Authority is therefore requested to issue SIGARM to the Civil Aeronautics Administration. The Chief Signal Officer would require the Civil Aeronautics Administration to account for all copies received.

FOR THE CHIEF SIGNAL OFFICER:

X-REFERENCE FILED IN:
450
Code-WDTC-SIGARM
3 Agencies-Non-Military

W. Preston Corderman
W. PRESTON CORDERMAN
Colonel, Signal Corps
Chief, Signal Security Branch

[redacted]

[redacted]

1st Ind.

Military Intelligence Division, WDGS, Washington 25, D. C., 5 June 1945

TO: The Chief Signal Officer, Washington 25, D. C.
(Attention: Signal Security Branch)

Request made in paragraph 4, basic communication is approved.

FOR THE ASSISTANT CHIEF OF STAFF, G-2:

Carter W. Clarke

CARTER W. CLARKE
Brigadier General, GSC
Deputy Chief, MIS

74

[redacted]

CONFIDENTIAL [redacted]

SPSIS 461 Codes
(12-22-42)

WAR DEPARTMENT
HEADQUARTERS, SERVICES OF SUPPLY
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON, D. C.

SPSIS-3

December 22, 1942.

MEMORANDUM TO: Lieutenant Colonel Cook

SUBJECT: Report on Cryptographic Security in the Division of Territories and Island Possessions, Department of the Interior.

1. It is necessary that the Division possess a means of confidential communication for use between Washington and Puerto Rico, the Virgin Islands, Alaska, Hawaii, and Seattle, Washington. Lateral communication is not necessary. The present means are the M-138-A strip device, used with a 30 alphabet set of strips and a daily change key list of 50 keys. This system was supplied by the Signal Security Service and has been in effect since July, 1942.

2. Investigation disclosed the following facts: a. Since each office possesses the same set of strips and uses the same key on any given day, it is believed that the system has reached the saturation point.

b. Personnel having access to cryptographic materials have not been properly investigated.

c. Numerous copies are made of both outgoing and incoming messages. These copies are not paraphrases, but are the original literal plain text.

d. Beginnings and endings of messages show much evidence of stereotypic form.

e. There exists within the Division no written regulations for the safeguarding of cryptographic security.

f. The combination of the Code Room safe has not been changed in "about five years".

3. The following corrective measures are being taken: a. A new set of alphabet strips with accompanying key list is being prepared for each field office. Each office will be furnished a different set of strips and key list in order to obviate the possibility of compromise of the entire system due to a loss of security at one point.

CONFIDENTIAL [redacted]

[redacted]

Memo to: Lt. Col. Cook SPSIS-J

b. Steps are being taken to instigate an investigation of key personnel by the F.B.I.

c. A manual of cryptographic security regulations has been prepared for distribution under the signature of the Director of the Division. This manual covers the following subjects:

(1) Marking of confidential messages.

(2) Dissemination of confidential information.

(3) Drafting of messages.

(4) Paraphrasing messages.

(5) Method of handling outgoing messages.

(6) Method of handling incoming messages.

(7) Principal dangers to cryptographic security.

(8) Storage of confidential messages and cryptographic documents.

d. Letters are being written to the Signal Officer in Puerto Rico, the Virgin Islands, Alaska, Hawaii, and Seattle, requesting that they send a qualified officer to the local office of the Division of Territories and Island Possessions for the purpose of assisting those offices in attaining a high degree of cryptographic security. The Director of the Division has welcomed this offer of assistance to the field offices and will direct them to cooperate with the Signal Corps in all matters pertaining to cryptographic security.

James G. Noak

James G. Noak
1st Lieutenant, Signal Corps

[redacted]

276

[redacted]

ROUTING AND WORK SHEET

(PAR. 42 O.R.)

SUBJECT: Cryptographic System for Rubber Development Corporation.

NUMBER EACH ACTION	TO	MEMORANDUM	NAME, DIVISION OR BRANCH, AND DATE
1.	Capt. Chittenden	1. Request that a strip system consisting of instructions, 100 alphabets, and Key List for 6 months (no channel elimination) be produced for use by the Rubber Development Corporation.	
		2. It is further requested that 12 copies of each item and 12 strip cipher devices be delivered in one package to Mr. Edward L. Stuhrman, Chief of Communications, Rubber Development Corporation, Room 211, 1626 K Street, N. W., Washington, D. C.	
		3. It is recommended that delivery be accomplished by May 6, 1943.	James G. Hoak Capt., Signal Corps SPSIS April 24, 1943
2.	Capt. J. G. Hoak	Production has been instructed to complete as stated, and in compliance with the information contained in the [illegible]	[illegible]

[redacted]

ROUTING AND WORK SHEET

(PAR. 40.62 OCR)

SUBJECT: Cryptographic material for Office of Scientific Research and Development

Number each action	To	Memorandum	Name, Division or Branch, and Date
1.	Major Chittenden	1. It is requested that Dr. William A. Shurcliff, Technical Aide, OSRD Liaison Office, Room 724, Dupont Circle Building, Washington, D. C., be furnished the following cryptographic material: a. 10 copies of an alphabet set of 100 strips. b. 5 copies of a key list for one year using a different key for each day of the year. c. 5 copies of instructions in the use of the above material. d. 10 devices CSP 845. 2. This system should be classified as SECRET, however the split generatrix should be employed instead of channel elimination. 3. This material should be delivered to CSRD not later than 8 January 1944.	James G. Noak Captain, SPSIC 18 December 1943 Ext. 263
2.	Captain James G. Noak	Material requested in Action 1 was delivered 7 January 1944.	Thomas R. Chittenden Major, SPSIC-2 15 January 1944 Ext. 269

SECRET

78

12-1600 29

[redacted]

HEADQUARTERS
ARMY SECURITY AGENCY
WASHINGTON 25, D. C.

SECRET
Security Information
Control Office
Date
NAV 3 Oct 46
OCT 3 1946

185

WDGAS-82

SUBJECT: Cryptosystem for Foreign Liquidation Commission

TO: Director, Army Security Agency, Pacific
APO 500, c/o Postmaster
San Francisco, California

1. It has come to the attention of this Agency that the cryptographic holdings of the Australian Base Command at Sydney have been reduced to the point where only M-209 and strip systems are held.

2. The Foreign Liquidation Commission has a representative at Sydney and messages addressed to him must be routed through the Australian Base Command. The use of M-209 or strip systems requires paraphrasing by the Base Command before delivery to the Foreign Liquidation Commission representative, as well as paraphrasing by the War Department Code Center before enciphering.

3. All other Foreign Liquidation Commission representatives are located at places where communication to them can be effected by means of Category A systems. In order to permit a similar situation at Sydney, it is proposed to provide your headquarters with a one-time-pad system for redistribution to the Australian Base Command. Upon receipt of concurrence from your headquarters, the necessary pads will be issued.

BY ORDER OF COLONEL BICHER:

Hamilton Jones

HAMILTON D. JONES
Major, Signal Corps
Executive Officer, ASA

[redacted]

3 Oct 46

82-1600-29

[redacted]

BASIC: Ltr fr Hq. Army Security Agency, Washington 25, D.C., dtd 3 Oct 46, subj: "Crytosystem for Foreign Liquidation Commission."

1st Ind.

HEADQUARTERS, ARMY SECURITY AGENCY, PACIFIC, APO 500, 15 October 46

TO: Chief, Army Security Agency, The Pentagon, Washington 25, D.C., ATTN: WDGAS-82

1. Information received at this headquarters indicates that the Australian Base Command will be deactivated prior to 31 December 1946. This deactivation date is an extension of the originally scheduled date of September 1946.

2. November and December editions of M-209 and strip systems are being distributed to the Australian Base Command at the specific request of that headquarters. The courier officer will depart from Tokyo on or about 18 October.

3. Inasmuch as it is believed that this will be the last courier trip to Australia, it has been deemed advisable to include a one-time-pad system, taken from stocks at this headquarters, in the distribution. The corresponding pads of the system provided are being forwarded to your headquarters for re-issue to the War Department Code Center. It is believed that less delay in providing facilities for the Foreign Liquidation Commission will be effected by this procedure.

FOR THE DIRECTOR:

RUSSELL H. HORTON
Lt. Colonel, Signal Corps
Assistant Director

[redacted]

260

Foreign - Non-Military

WAR DEPARTMENT [redacted] RA. SMITTAL SHEET

ARMY SERVICE FORCES

Action 1

TO	(Service, division, or organization)	(Location)
	OIC, Operations Section (Branch or unit)	(Attention)
Subject:	Standard Form for Documents Prepared for Federal Agencies	
File No.	SPSIC-6 (Writer's last name)	12 February 1945 (Date)
FROM:	(Service, division, or organization)	RIH, Ext 449 (Location) (Telephone extension)

Standard forms for cryptographic documents prepared for various federal agencies and UNRRA have been recommended by the Plans and Operations Staff. These forms, which incorporate the details indicated below, are approved. All future documents prepared for federal agencies and for UNRRA should be prepared accordingly.

a. Documents will be prepared without the usual headings, e.g., "War Department", "Army Service Forces", "Combined Communications Board", etc.

b. War Department authentication will not be used.

c. Documents prepared for issue to various agencies:

(1) Will bear long and short titles, the latter consisting of the root, "FED" followed by letters and numerals which identify individual documents and the respective edition thereof, e.g., "Instructions for Using the Strip Cipher" would bear the short title FEDB-1.

(2) Will contain a statement as follows: "Prepared under the supervision of the War Department for authorized federal agencies."

(3) Will designate the "Distributing Agency" (i.e., the respective federal agency) as the office of record.

d. Documents prepared for issue to a specific agency:

(1) Will bear long and short titles, the latter consisting of the root, "FED" followed by the abbreviation of the respective federal agency and numerals which identify individual documents, e.g., "OWI Cipher Key List No. 200" would bear the short title FEDOWI-200.

(2) Will contain a statement as follows: "Prepared under the supervision of the War Department for the _____________*."

* Example: The Office of War Information.

X-REFERENCE FILED IN:
1. Documents-Publication
2.
3.

W.D., A.G.O. Form No. 0105
March 27, 1943

[redacted]

[redacted]

(3) Will designate the respective agency as the office of record

* Example: Office of [redacted]

e. Documents prepared for UNRRA will incorporate the details contained in sub-paragraphs a, b and d(2) and (3) above. Short titles for these documents will consist of the letters UNRRA followed by identifying numerals and letters, e.g. "Literal One-Time Pad UNRRA-60" will bear the short title UNRRA-60. Superseding editions of this pad will use the short title UNRRA-60A, UNRRA-60B, etc.

K. Kuhn
Lt. Col., Signal Corps
SPSIC; Ext 210

[redacted]

Agencies – Non Military

CSGAS-82 23 August 1948

SUBJECT: Report of Contacts Outside of Security Division

TO: Chief, Security Division
Chief, Technical Staff
Chief, Methods Branch
Civilian in Charge, Central Files
IN TURN

Organization visited: Cryptographic Aids Committee

Persons contacted: Captain Gorgie, Navy Department; Commander Hargreaves, Navy Department; and Mr. Anderson, State Department

Subjects discussed: Type of Cryptographic Aids to be Furnished Nonmilitary Federal Agencies and Cryptographic Aids for Panama Canal

Results of discussion including commitments made:

1. A meeting was held by the Cryptographic Aids Committee to discuss general cryptographic facilities that should be made available to nonmilitary federal agencies which, in the future, might be authorized crypto-systems. Discussion resolved that, barring exceptional circumstances, such agencies would be limited to one-time pads, one-time tapes, strip systems and running key ciphers, dependent on volume of traffic, speed requirements, personnel clearances and security of the installations concerned. It was agreed that in such cases, if one-time pads should be employed, the Army would be responsible for production. If running ciphers were to be employed, the Department of the Navy would be responsible. Operating instructions were to be, generally speaking, in accordance with JANAP 122.

2. Consideration was further given to cryptofacilities presently employed by the Panama Canal office. The Panama Canal office had been issued a strip system nine years ago for use between its Washington office and parent headquarters. Although no use had been made of this system in the last several years, it had been the feeling of Mr. Burdick of the Panama Canal office that, despite lack of current need for the system, it should be retained by that office for emergency purposes. It was the opinion of the Committee that the existing strip system would be of little security in the event it actually had to be used since there had been no changes whatsoever in the system in nine years. It was therefore decided that, after further check with the Panama Canal office, substitution of one-time pads should be made for this system.

23 Aug 48

CSGAS-82 23 August 1948

Subject: Report of Contacts Outside of Security Division

Recommendation and/or action taken:

1. That nonmilitary federal agencies authorized cryptosystems by the Cryptographic Board should, under normal conditions, be issued either one-time pads, one-time tapes, strip systems or running key ciphers.

2. That, in the specific instance of the Panama Canal office, their current strip system should be replaced by one-time pads if subsequent investigation indicated a small number of holders and adequacy of this system.

W. V. RUSSO
Chief, Material Branch

THE COMBINED CHIEFS OF STAFF
WASHINGTON
25 DC

COMBINED COMMUNICATIONS BOARD

26 May 1943

MEMORANDUM FOR: Assistant Chief of Staff, Operations Division, WDGS (Maj. Gen. T. T. Handy)

THROUGH: U.S. Secretary, Combined Chiefs of Staff

Subject: Issue of Combined Cryptographic Systems to Allied Forces other than U.S. - British

1. The Combined Communications Board recommends that the following rules be promulgated by your Service to govern the issue of combined cryptographic systems to Allied forces other than U.S. - British:

a. A combined cryptographic system authorized for issue to Allied forces actively engaged in military, naval or air operations should be released to such forces by personnel of liaison units, consisting of either U.S. or British personnel, when authorized to do so by the U.S. or British commanders concerned.

b. This authorization shall only be given in cases where covering permission to issue the publication under consideration to forces of the nation in question has already been granted.

c. In the case of Combined Communications Board publications, such covering permission will be granted by the C.C.B.

d. The documents or extracts therefrom shall be issued as near the time at which they come into use as possible, and shall be effective for as short a period as is practicable.

e. Wherever possible special editions of code books and/or cipher keys should be issued.

f. The following is a list of combined cryptographic systems approved by the C.C.B. which may be issued to Allied Forces when they are engaged in active operations:

[redacted]

Combined Field Code
Self Evident Code — Lettered Coordinates
Syko — RECKON
Aircraft Reporting Code
Authenticator System, Air-to-Ground only
Fighter Director Vocabulary

f. The following is a list of combined cryptographic systems which may not be issued to Allied Forces:-

Type X (Limited Combined)
Naval Cipher #3 (Limited Combined)
CCM
Strip Standby for CCM
Authenticator Syatem, point to point

2. This information is furnished for necessary action by the War Department and a similar memorandum is being addressed to the Navy Department.

(S. 30)

R. L. WALKER
Lt. Col., AUS
Deputy U.S. Secretary

Copy to:
Col. W. T. Sexton,
Secretary, WDGS

1st Ind.

U.S. Secretary, Combined Chiefs of Staff, Washington, D.C.
27 May 1943.

To: Assistant Chief of Staff, Operations Division, WDGS
(Maj. Gen. T. T. Handy)

Forwarded for necessary action.

G. B. MYERS,
Commander, U.S. Navy
Assistant U.S. Secretary
Communications

Copy for
Accompany original

[redacted]

[redacted]

Issue of Combined Cryptographic Systems to Allied Forces other than U. S. and British

1. Forwarded for necessary action and compliance with the attached Disposition Form.

2. If this information is to be directed to other War Department agencies, you will prepare the necessary letter or circular to be issued by The Adjutant General, together with recommended dissemination. The recommended dissemination will include those agencies enumerated in Paragraph 3 of the Disposition Form and the Combined Communications Board.

3. If this information is to be furnished to Theaters of Operation, you will prepare the necessary message to be dispatched by The Adjutant General.

4. Attention is invited to Paragraph 2 of the Disposition Form, the substance of which should be included in the letter to The Adjutant General.

5. You will prepare a memorandum to the Assistant Chief of Staff, Operations Division, War Department General Staff, Attention Combined Subjects Section, attaching four copies of the action taken. One copy of the action taken will be forwarded to the Director of Planning, OCSigO.

6. Correspondence to higher authority relative to the attached decision will be prepared for signature of the Executive Officer, and a copy will be furnished for the Executive Office files.

1 Incl.
DF fm OPD dtd 28 May 1943
re above w/incl cy of CCB memo
dtd 26 May 1943.

Director
Signal Security
Division

Wm D. Hamlin
Colonel, SPSIO-1
Executive
Br. 71279
31 May 43

[redacted]

8

SECRET

Issue of Combined Cryptographic Systems to Allied Forces other than U. S. and British (Cont'd)

2 Executive Officer OCSigO — The necessary action has been taken.

1 Incl. w/d

Charles H. Hiser
Major, Signal Corps
Sig. Sec. Serv.
11 June 1943

SECRET

Copy

"SECRET"

U.S. Military Mission
American Embassy
San Jose, Costa Rica

24 April 1944

SUBJECT: Cryptographic Systems

TO: Assistant Chief of Staff, G-2
(Att. Collection Unit)
War Department, Washington, D.C.

1. The Military Mission to Costa Rica is making extensive recommendations to the government for the organization of its Army along modern lines including an intelligence and communications service. It is desired to provide at least an elementary cryptographic system.

2. It is believed that certain cryptographic practices and equipment in use by the United States for confidential communications which are based on an arbitrary pre-arranged code, such as the aluminum disc set, could be utilized by the Costa Rican Army without prejudice to the security of the United States.

3. The writer is reluctant to undertake to improvise a rudimentary cryptographic system and offer it to the Costa Rican government without complete instructions.

4. If it is considered proper to make recommendations to the Costa Rican government for a cryptographic system embodying the mechanics of U.S. Army systems, it is believed preferable that I be provided with the specific matter which can be disclosed.

/S/ JESS C. RADNOR
Jess C. Radnor
Lieutenant Colonel, C.A.C.
Chief of Mission

"SECRET"

Copy

90

Authorization Request for instructional material to C.R. 2725

[redacted]

G-2

Subject: Cryptographic Systems.

6 May 1944.

X CSO

Attention: Signal Security Agency.

X-REFERENCE FILED IN:
1. 450
2. M-94
3. FM 24-5

X Remark and recommendation

---

1. Reference is made to the attached letter dated 24 April 1944 from the Chief of the U. S. Military Mission, Costa Rica, subject as above.

2. It is believed to be undesirable to furnish the Costa Rican Government with information concerning current U. S. Army Cryptographic systems. However, it is believed that no threat to security would arise as a result of furnishing the Costa Rican Government with information and instructional material on the M-94 system to serve as an example of a cryptographic system for field use in the reorganized Costa Rican Army.

3. It is not considered desirable to place the War Department in the position of offering to equip the Costa Rican Army with such cryptographic devices and instructional material.

4. If your office is in agreement with the point of view expressed above, it is requested that sufficient informational material be furnished to this Division, for forwarding to the Chief of the U. S. Military Mission to Costa Rica, to meet the requirements indicated in paragraph 4 of reference letter.

For the A. C. of S., G-2:

CARTER W. CLARKE,
Colonel, General Staff Corps,
Assistant Executive Officer, G-2.

Incl.
Ltr dtd 24 Apr 44 fr
MM Costa Rica.

[redacted]

[redacted]

SUBJECT: Cryptographic Systems

SPSIC 461 Codes
(6 May 1944) 1st Ind. SPSIC-b

ASF, OCSigO, Washington 25, D. C., 13 May 1944

TO: Assistant Chief of Staff, G-2, Room 2E728, The Pentagon, Washington 25, D. C. Attention: Colonel Clarke

1. The Signal Security Branch is in agreement with the point of view expressed in the basic communication.

2. Inclosed is a copy of FM 24-5, Signal Communication. Attention is invited to paragraphs 50-57, which describe the operation of the M-94 Cipher device. This material can be forwarded to the Chief of the U. S. Military Mission to Costa Rica.

For the Chief Signal Officer:

W. Preston Corderman
Colonel, Signal Corps
Chief, Signal Security Branch

2 Incls.
Incl 1. n/c
Added 1 Incl.
Incl 2. FM 24-5,
Signal Comm.

[redacted]

[redacted]

Cryptographic Material for French Troops

1: Chief, Signal Security Agency

1. Attention is invited to the attached radio.

2. It is suggested that authority be given this office to issue a special strip system and a special M 209 system to this French corps. These systems could be prepared in four days time. If proper authority is received by 16 September this office will have sufficient time in which to prepare and deliver the systems and devices to AFHQ Algiers by 5 October 1943.

3. The cryptographic materials involved would be:

a. The Instructions for Operating Strips Systems (short title: SIGUHR)

b. Keying Instructions for the Converter M 209

c. The strips cipher device type M 138 A or CSP 845

d. The converter M 209

e. Special strip systems and special M 209 systems.

4. The instructions for operating strip cipher systems have been translated into French and are immediately available in that form. Keying and operating instructions for the M 209 have not been translated to the best of our knowledge.

5. Instructions for use of double transposition systems (short title: SIGCRED-2) are in the process of being translated into French at present. However, the length of time required to encipher by means of double transposition is prohibitive for a tactical situation. Therefore, supplying of a double transposition system has not been recommended for this operation.

1 Incl
Incl: M-209 Radio AS-NR 6565

Clinton B. [illegible]
Colonel, Sig. C[illegible]
SPSIC 2 Sept. [illegible]
Ext. 2/1

[redacted]

ARMY

[redacted]

WAR DEPARTMENT
ARMY SERVICE FORCES
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON 25, D. C.

IN REPLY REFER TO
SPSIC 161 Codes

SPSIS
30 October 1943

Subject: Supply of Cryptographic Material to Italian Army

To: Assistant Chief of Staff, G-2, War Department General Staff, War Department, Washington 25, D. C.

1. A request has been received from Allied Force Headquarters, Algiers, for cryptographic material to be supplied to units of the Italian Army and Air Force. This request is contained in secret radio W 3444 26 October 1943 (CM-IN-15803-26 Oct 1943).

2. Paragraph 2d of letter TAG, 24 March 1943, file AG 312.11 (3-19-43) AB-S-B-M, Subject, Access to Cryptographic Material, prohibits the issuance of cryptographic systems to any other nation unless prior specific authorization is obtained from the War Department in each instance.

3. The cryptographic materials involved would be:

a. The Instructions for operating Strip Systems (short title SIGUHR).

b. The strip cipher device CSP 845 or SIGWOMO alphabet.

c. Special strips and key lists.

4. According to the radio from Allied Force Headquarters, the translation of the instructions for using strip systems is being accomplished at that headquarters.

5. It is requested that authorization be given this office to produce and issue this cryptographic material to units of the Italian Army and Air Force.

For the Chief Signal Officer:

W. Preston Corderman
Colonel, Signal Corps

[redacted]

SECRET

MID 911 1st Ind.

G-2, W.D.G.S., Washington 25, D. C., 4 November 1943.

To: Chief Signal Officer, War Department, Washington 25, D. C.
Attention: Signal Security Agency.

1. With reference to paragraph 3, basic communication, authorization is given hereby to furnish AFHQ with special cryptographic material for distribution to units of the Italian Army and Air Force.

2. In accordance with paragraph 2 d., TAG letter dated 24 March 1943, file AG 312.11 (3-19-43)OB-S-B-M, subject: Access to Cryptographic Material, a message has been sent to the Commanding General, AFHQ, authorizing the issuance of this special cryptographic material to units of the Italian Army and Air Force.

GEO. V. STRONG,
Major General,
A. C. of S., G-2.

SECRET

[redacted]

CROSS-REFERENCE SHEET

FILE UNDER: Authorization Request Transfer of Mat. AG-G-2

DATE OF CORRESPONDENCE: 2 Oct 45

TYPE OF CORRESPONDENCE:

✓ RADIOGRAM AS CM-IN 631 WD OUT 23974

___ LETTER ___ INDORSEMENTS

___ TRANSMITTAL ___ ACTIONS

___ R AND W ___ ACTIONS

___ TRANSFER FROM ______ TO ______

___ MEMORANDUM

SYNOPSIS:

Cryptographic material held by Philippine Army as follows: Sig HR-3, Sig AED-2, Sig P.F. + M209 Sigs.
Recommend Office of Record this Theater retain full accountability & continue to require all normal reports from Philippine Army.

PAPERS FILED UNDER: 785 - Pacific Theater

96

FORM NO. 498
1 OCTOBER 1944 [redacted] 2 Oct 45

[redacted] 8589

8 January 1944

MEMORANDUM TO: Assistant Chief of Staff, G-2

SUBJECT : Cryptographic Systems for Russian Armed Forces

1. In compliance with paragraph 3 of a directive from the Joint Communications Board dated 30 December, Subject: "Release of Communications Equipment and Related Technical Information to the U.S.S.R.", a copy of which is inclosed, it will be necessary for the Joint Codes and Ciphers Committee to prepare a list of cryptographic systems which may be issued when necessary to the Russian Armed Forces. The following list of cryptographic systems are recommended for this category:

a. Strip Systems

b. M-209 Systems

c. One-time Pad Systems

d. Subtractor Tables for Meteorological Codes

e. Alnco

f. Authentication Systems Prescribed for use below division.

2. In all cases it is contemplated that special key-lists and/or strips in the case of strip systems will be issued.

3. It is requested that the above list be approved in order that it may be submitted by this office to the Joint Codes and Ciphers Committee for inclusion in their report to the Joint Communications Board.

4. It is requested that the inclosure be returned to Signal Security Agency.

For the Chief Signal Officer:

(W. Preston Corderman)
W. Preston Corderman
Colonel, Signal Corps

1 Incl:
JCB Directive dtd
30 Dec 43

[redacted]

[redacted] 59

WAR DEPARTMENT
WAR DEPARTMENT GENERAL STAFF
MILITARY INTELLIGENCE DIVISION G-2
WASHINGTON

13 January 1944.

MEMORANDUM FOR THE CHIEF SIGNAL OFFICER:
(Attention: Signal Security Agency)

Subject: Cryptographic Systems for Russian Armed Forces.

1. Reference is made to your memorandum of 8 January 1944, subject as above, a copy of which is inclosed.

2. The request contained in paragraph 3 of reference memorandum is approved.

3. As requested in paragraph 4 of reference memorandum, the JCB Directive dated 30 December 1943, subject: Release of Communications Equipment and Related Technical Information to the U.S.S.R. is returned herewith.

For the A. C. of S., G-2:

CARTER W. CLARKE,
Colonel, General Staff,
Assistant Executive Officer, G-2.

2 Incls:
Incl #1-cy Memo dtd 8 Jan 44.
Incl #2-JCB Directive.

FOR VICTORY BUY UNITED STATES WAR BONDS AND STAMPS

[redacted]

8989

[redacted]

21 January 1944

SPSIC 461 Codes

MEMORANDUM TO: Assistant Chief of Staff, G-2
Attention: Major Goodrich

SUBJECT: Cryptographic Systems for Russian Armed Forces.

Attention is invited to the attached memorandum dated 8 January 1944 subject: "Cryptographic Systems for Russian Armed Forces". It is requested that the cryptographic systems listed in paragraph 1 of the subject memorandum be amended to include as item g, "Double Transposition Systems."

For the Chief Signal Officer:

(W. Preston Corderman)
W. Preston Corderman
Colonel, Signal Corps

1 Incl.
Memo, 8 Jan 44 to A. C. of S, G-2

COPY

CT-152 8989

WAR DEPARTMENT
WAR DEPARTMENT GENERAL STAFF
MILITARY INTELLIGENCE DIVISION G-2
WASHINGTON

26 January 1944

MEMORANDUM FOR THE CHIEF SIGNAL OFFICER
(Attention: Signal Security Agency)

Subject: Cryptographic Systems for Russian Armed Forces.

1. Reference is made to your memorandum of 21 January 1944, subject as above, a copy of which is inclosed.

2. The request contained in reference memorandum is approved.

For the A. C. of S., G-2:

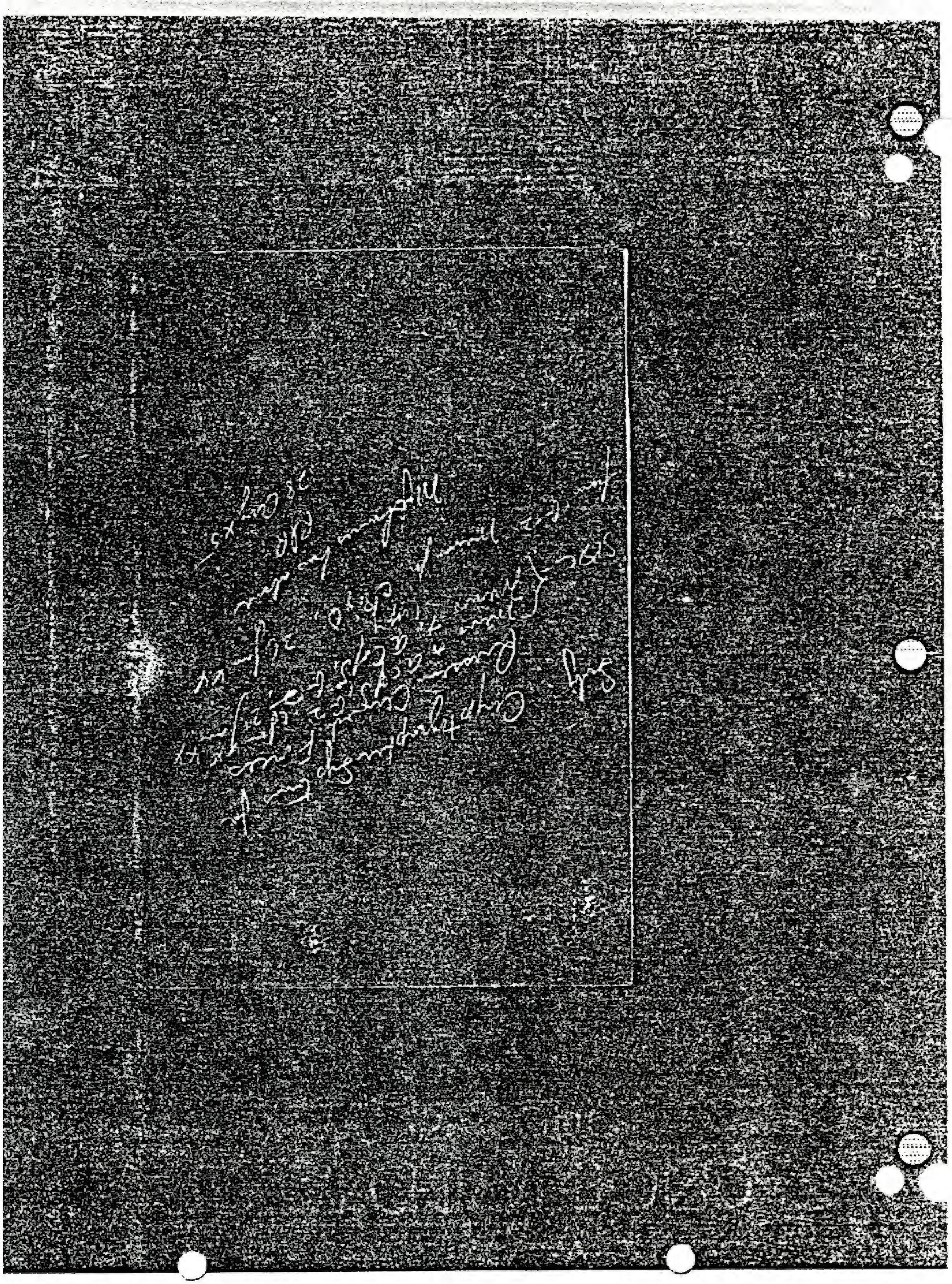
CARTER W. CLARKE,
Colonel, General Staff,
Assistant Executive Officer, G-2.

2 Incls:
Incl #1-Cy Memo dtd 21 Jan 44
Incl #2-Cy Memo dtd 8 Jan 44

1-26-44

FOR VICTORY BUY UNITED STATES WAR BONDS AND STAMPS

[redacted]



SECRET

CROSS-REFERENCE SHEET

FILE UNDER: [illegible]

DATE OF CORRESPONDENCE: 8 Feb 45

TYPE OF CORRESPONDENCE:

- ___ RADIOGRAM
- ___ LETTER
- ✓ TRANSMITTAL
- ___ R AND W
- ___ TRANSFER FROM ___ TO ___
- ___ INDORSEMENTS
- 3 ACTIONS
- ___ ACTIONS

SYNOPSIS: [illegible]

[illegible]

PAPERS FILED UNDER: [illegible]

SECRET

SAVE

SECRET

ARMY SERVICE FORCES
SIGNAL SECURITY AGENCY
WASHINGTON 25, D. C.

Secret
By ... of the ... Union
Initial ... Date

SPSIS-3

18 August 1945

SUBJECT: Furnishing U. S. Army Cryptographic Systems to Russia.

TO: Commanding General
Signal Security Agency

1. Note the following extracts from Security Division daily reports:

"A member of this Branch contacted G-2 to make tentative arrangements for translation of strip cipher or double transposition instructions into Russian and to get an estimate on the time required. This was done at the request of Cryptographic Materiel Branch."

"The European Theater has been notified that the original objection to the use of a Russian strip system for United States--Russian traffic in the Allied occupational zones in Europe has been withdrawn. This decision was made after receipt of information from the theater that only letters, numerals, and punctuation which can be transmitted by American radio operators will be used in this traffic. Our original objection was based on the production and operational difficulties involved in a strip system employing the thirty-character Russian alphabet. Subject to final approval from the Theater, a Russian translation of the strip cipher instructions and stencils also in Russian for use as master copy in the production of monthly key lists will be furnished. The translations will not be started until the theater concurs."

"A draft of "Instructions for Using the Strip Cipher Device" (short title: SIGWHIT-I) was taken to G-2 for translation into Russian."

2. According to Major Innes of Cryptographic Materiel Branch, these systems have been requested by Colonel Cook of SID, USFET.

SECRET

SPSIS-3 (18 August 45)

3. The furnishing of such systems seems to be in line with previous policy of furnishing the French and other Allies with U.S. systems for joint use. I have always questioned this policy and would prefer to see the others furnish their systems to us after first making necessary security changes. In the present case, I think it especially desirable to use a Russian system, and especially undesirable to furnish a U. S. system.

4. Perhaps this is a matter that should be discussed with G-2 and ANCCIC.

MARK RHOADS
Assistant Director of
Communications Research

ARMY SERVICE FORCES
SIGNAL SECURITY AGENCY
WASHINGTON 25, D. C.

1. Customary to use our systems in other allied use. (France, Italy, Brazilians)

2. Translations of reg. UHR made in French & Italian (Brazilians used O.T. Pads.

3. Hayes prefers we use our systems and not the Russians

4. G-2 has approved

SECRET CONFIDENTIAL RESTRICTED

TO DATE FR

Commanding General (IS-1)
Executive Officer (IS-1)
Dir of Comm Research (IS-3)
Control O (IS-1A)
Fiscal O (IS-1B)
Administrative O (IS-2)
Post Adjutant (IS-2)
Intelligence O (IS-2)
Provost Marshal (IS-2)
2d Sig Serv Bn (IS-6)
Chief, Pers & Tng Div (IS-4)
Chief, Pers Br (IS-4A)
Chief, Tng Br (IS-4B)
Chief, O Pers Sec (IS-4C)
Chief, Oper Serv Div (IS-5)
Chief, Comm Br (IE)
Chief, Lab Br (ID)
Chief, Machine Br (IN)
Chief, Supply Br (IS-5A)
O/C SSA Mail Unit (IE-2C)
Chief, Security Div (IS-8)
Chief, Prot Sec Br (AP)
Chief, Crypt Mat Br (IC)
Chief, Equipment Br (IF)
Chief, Comm Sec Br (IS-8A)
Chief, Intelligence Div (IS-9)
Chief, Lang Br (IB-1)
Chief, Mil Crypt Br (IB-2)
Chief, Gen Crypt Br (IB-3)
Chief, T/A and C Br (IB-4)
Chief, I & L Br (IR)

As discussed
As requested
Comments and return
Information and file
Information and forwarding
Information and return
Recommendation
See note on reverse
Signature if approved
Your action

We shall proceed with the original plan. Enclosure is returned herewith.

SIS SC Form No. 96 (Rev 5)
2 July 1945

SECRET CONFIDENTIAL RESTRICTED

TO DATE 7 Sept 45 FROM

- Commanding General (IS-1) ✓
- Executive Officer (IS-1)
- Dir of Comm Research (IS-3)
- Control O (IS-1A)
- Fiscal O (IS-1B)
- Administrative O (IS-2)
  - Post Adjutant (IS-2)
  - Intelligence O (IS-2)
  - Provost Marshal (IS-2)
  - 2d Sig Serv Bn (IS-6)
- Chief, Pers & Tng Div (IS-4)
  - Chief, Pers Br (IS-4A)
  - Chief, Tng Br (IS-4B)
  - Chief, O Pers Sec (IS-4C)
- Chief, Oper Serv Div (IS-5)
  - Chief, Comm Br (IE)
  - Chief, Lab Br (ID)
  - Chief, Machine Br (IN)
  - Chief, Supply Br (IS-5A)
  - ✓ O/C SSA Mail Unit (IE-2C)
- ✓ Chief, Security Div (IS-8) MBJ
  - Chief, Prot Sec Br (AP)
  - ✓ Chief, Crypt Mat Br (IC)
  - Chief, Equipment Br (IF)
  - Chief, Comm Sec Br (IS-8A)
- Chief, Intelligence Div (IS-9)
  - Chief, Lang Br (IB-1)
  - Chief, Mil Crypt Br (IB-2)
  - Chief, Gen Crypt Br (IB-3)
  - Chief, T/A and C Br (IB-4)
  - Chief, I & L Br (IR)

- As discussed
- As requested
- Comments and return
- Information and file
- Information and forwarding
- Information and return
- Recommendation
- See note on reverse
- Signature if approved
- Your action

Since Gen Clarke wants to continue using joint systems made up by Americans we should go ahead with present plans.
a.k.

SIS SC Form No. 96 (Rev 5)
2 July 1945

Authorization for Issuance of Material

ARMY SERVICE FORCES
SIGNAL SECURITY AGENCY
WASHINGTON 25, D. C.

General Corderman

1. General Clarke authorized the use of our methods (systems) and translated instructions for inter-allied messages and Russian in particular on 26 Jan 44.

2. The contrary decision of ANCICC was brought to Gen. Clarke's attention by Col. Goodrich.

3. Gen. Clarke according to verbal advice from Col. Goodrich has reconfirmed the decision of 26 Jan 1944.

4. We are proceeding with the preparation of the material Col. Cook requested unless I hear from you to the contrary.

SECRET

W. Jones

REFERENCE FILE No.
450
3
7528